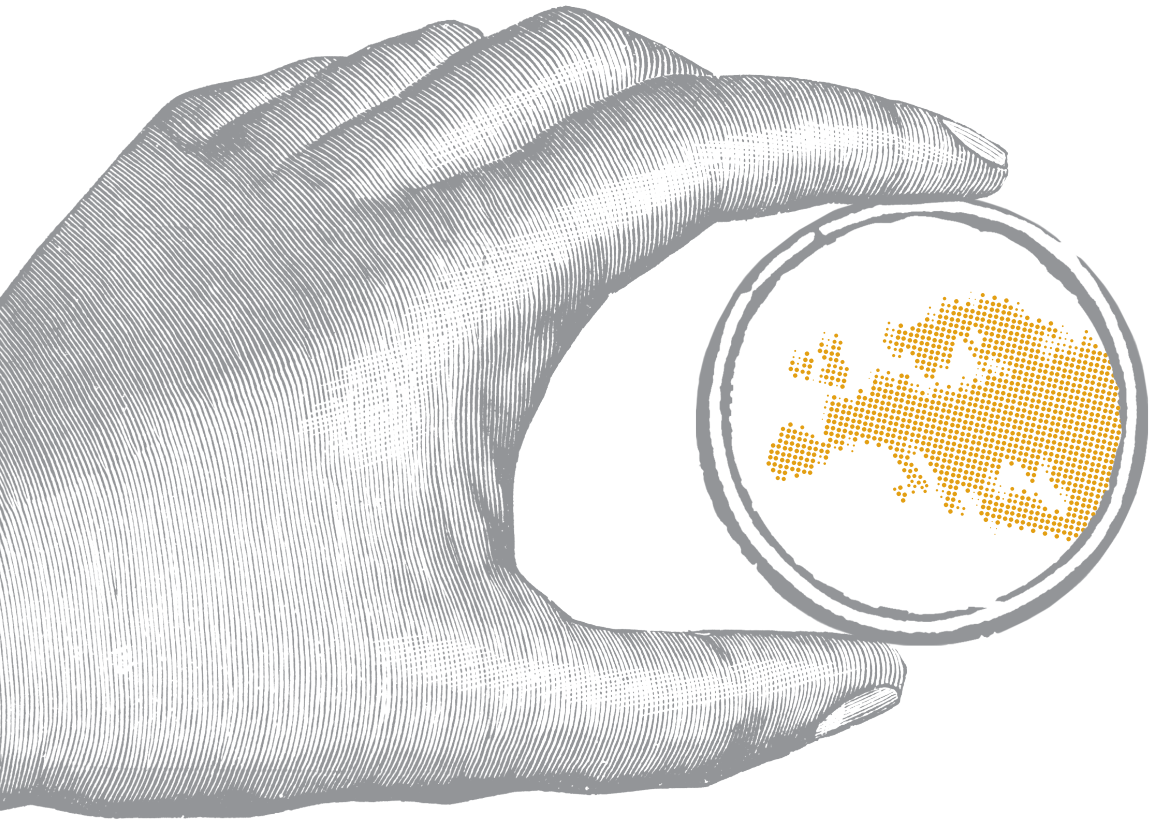
GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

CONTRIBUTI

APPLICARE IL GDPR

II volume

Le linee guida europee 2019-2022



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza Venezia n. 11 - 00187 Roma
Tel: +39 06.69677.1
Fax: +39 06.69677.3785
e-mail: protocollo@gpdp.it
posta certificata: protocollo@pec.gpdp.it

www.gpdp.it

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Applicare il GDPR

Le linee guida europee

II volume

www.gpdp.it

Sommario

Prefazione 9

I diritti degli interessati 11

Premessa - I diritti degli interessati 12

Linee guida 5/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca, ai sensi del RGDP (parte 1) - Versione 2.0 14

Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679 - Versione 1.1 34

Obblighi di titolari e responsabili - accountability 79

Premessa - Obblighi di titolari e responsabili - accountability 80

Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679 - Versione 2.0 86

Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati - Versione 2.0 122

Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0 144

Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita - Versione 2.0 184

Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità - Versione 2.0 224

Linee guida 06/2020 sull'interazione tra la seconda direttiva sui servizi di pagamento e il GDPR - Versione 2.0 270

Linee guida 07/2020 sui concetti di titolare del trattamento e responsabile del trattamento nel GDPR 302

Linee guida 8/2020 sul targeting degli utenti di social media - Versione 2.0 372

Linee guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali - Versione 2.0 428

Linee guida 02/2021 sugli assistenti vocali virtuali - Versione 2.0 474

Raccomandazioni 02/2021 sulla base giuridica per la conservazione dei dati delle carte di credito al solo scopo di agevolare ulteriori operazioni online 524

Decisione di esecuzione 2021/915 della Commissione europea – Clausole contrattuali tipo titolare-responsabile del trattamento 530

Requisiti aggiuntivi di accreditamento degli organismi di certificazione 548

Requisiti di accreditamento degli organismi di monitoraggio dei codici di condotta 574

Trasferimenti di dati verso paesi terzi e organismi internazionali 591

Premessa - Trasferimenti di dati verso paesi terzi e organismi internazionali 592

Linee guida 2/2020 sull'articolo 46, paragrafo 2, lettera a), e paragrafo 3, lettera b), del regolamento 2016/679 per i trasferimenti di dati personali tra autorità ed organismi pubblici del SEE e di paesi non appartenenti al SEE - Versione 2.0 596

Linee guida 4/2021 sui codici di condotta come strumento per i trasferimenti - Versione 2.0 620

Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE - Versione 2.0 642

Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza 700

Raccomandazioni 1/2021 sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie 718

Dichiarazione in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – Data Protection Commissioner contro Facebook Ireland e Maximillian Schrems 740

Domande più frequenti in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems 744

Decisione di esecuzione 2021/914 della Commissione europea – Clausole contrattuali tipo per trasferimenti dati verso paesi terzi 752

Meccanismi di applicazione del GDPR **785**

Premessa - Meccanismi di applicazione del GDPR 786

Linee guida 3/2018 sull'ambito di applicazione territoriale del RGPD (articolo 3) - Versione 2.1 788

Parere 8/2019 sulla competenza di un'autorità di controllo in caso di mutamento delle circostanze relative allo stabilimento principale o unico 828

Linee guida 9/2020 sull'obiezione pertinente e motivata ai sensi del regolamento (UE) 2016/679 - Versione 2.0 840

Covid-19 **859**

Premessa - Covid-19 860

Linee guida 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19 862

Linee guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 880

Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia da COVID-19 906

Appendice **913**

Riferimenti utili 914

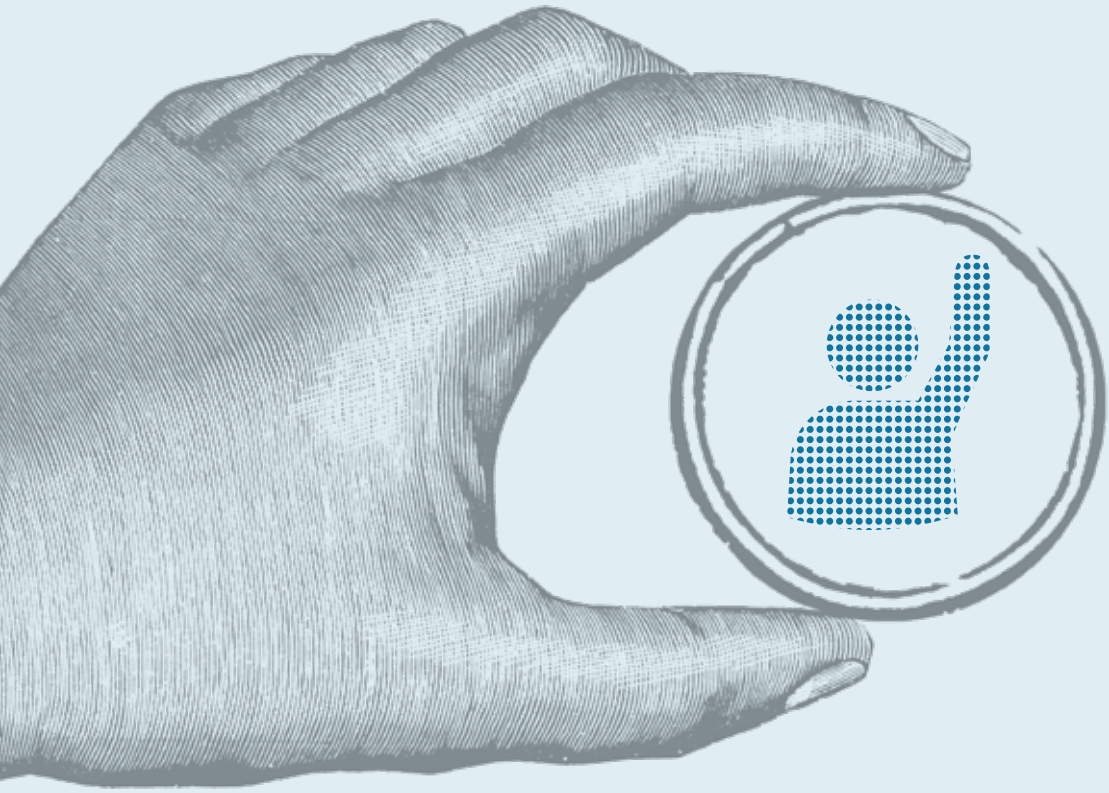
Prefazione

Con il secondo volume di "Applicare il GDPR", il Garante offre una panoramica completa dei documenti di indirizzo e orientamento prodotti dal Comitato europeo per la protezione dei dati fra il 25 maggio 2019 e la fine del 2022, per i quali è disponibile una versione definitiva (al netto, quindi, di consultazioni pubbliche o ulteriori perfezionamenti). L'obiettivo perseguito è lo stesso del precedente volume: fornire uno strumento agile e comprensivo, di consultazione e di riferimento, destinato in primo luogo a titolari e responsabili del trattamento, ma anche ai responsabili della protezione dei dati, chiamati ad assistere i primi nel dare attuazione adeguata e integrale alle norme del Regolamento europeo sulla protezione dei dati personali (il GDPR). Il volume offre, inoltre, chiarimenti e spunti di riflessione a tutti coloro che vogliano comprendere e tutelare meglio i diritti fondamentali alla privacy e alla protezione dei dati, che rappresentano strumenti di democrazia prima ancora che facilitatori dell'economia contemporanea.

L'arco temporale coperto da questa pubblicazione ha visto il manifestarsi di grandi sfide e problemi, non solo per la protezione dei dati, ma per la società nel suo complesso. In primis la pandemia di Covid-19, che ha reso necessario disegnare strumenti emergenziali di salute pubblica garantendo sempre il corretto bilanciamento fra diritti egualmente fondamentali, quali il diritto alla salute e quello alla tutela della propria sfera privata rispetto a ingerenze ingiustificate o eccessive. Su altri versanti, sono stati anni di intenso lavoro per il Comitato europeo e le autorità, che hanno avuto modo di confrontarsi su questioni applicative a tutto campo anche alla luce del sempre più prepotente emergere di tecnologie pervasive e complesse come l'intelligenza artificiale in tutte le sue declinazioni. Vale la pena aggiungere, in questa prospettiva, che numerosi sono stati gli sviluppi normativi e giurisprudenziali riferiti alla protezione dei dati negli ultimi anni, e che di tali sviluppi si coglie un riflesso anche nei documenti qui presentati.

Tutta la documentazione è rinvenibile sul sito del Comitato (www.edpb.europa.eu); il volume raccoglie anche alcuni provvedimenti del Garante, disponibili sul sito dell'autorità (www.gpdp.it), che integrano o specificano le prescrizioni o le raccomandazioni del Comitato. I documenti sono stati raggruppati in cinque macro-aree, le stesse del precedente volume (diritti degli interessati, obblighi di titolari e responsabili, principi relativi ai trasferimenti internazionali di dati personali, meccanismi attuativi del GDPR) oltre a una quinta, che si aggiunge alle precedenti, per dare conto delle attività a vario titolo connesse all'emergenza da Covid-19. Completano il volume una sezione contenente link e riferimenti utili, e un mini-glossario dei principali termini e acronimi utilizzati nei testi qui raccolti.

1 I diritti degli interessati



Premessa
I diritti degli interessati

Il RGPD ha, da un lato, rafforzato i diritti riconosciuti agli interessati e, dall'altro lato, ha introdotto nuovi diritti fra cui il diritto all'oblio.

Le **linee guida sul consenso** (aggiornate alla versione 1.1. del 4 maggio 2020) rappresentano, in questo senso, un esempio significativo. Pur essendo il consenso uno dei requisiti per trattare lecitamente dati personali e non (soltanto) un diritto degli interessati, il RGPD richiede uno sforzo di trasparenza maggiore da parte dei titolari soprattutto quando vogliano ricorrere al consenso per trattare dati personali. Quindi l'EDPB ha chiarito, in particolare, cosa debba intendersi per consenso realmente 'informato', e come si declinano gli obblighi di trasparenza (non solo di informazione) rispetto agli interessati, con particolare riguardo proprio alla prestazione del consenso, anche evidenziando la possibilità di alcune semplificazioni. Non si può dimenticare, infine, che molti dubbi hanno accompagnato e accompagnano l'applicazione del requisito di un consenso "esplicito" per il trattamento delle categorie particolari di dati personali di cui agli artt. 9 e 10 del RGPD, e anche su questo punto le linee guida offrono indicazioni operative ed esempi tratti dalla prassi quotidiana anche alla luce dei contributi giunti dalla consultazione pubblica indetta dall'EDPB.

Con le **linee guida 5/2019 in tema di diritto all'oblio** (più correttamente, alla cancellazione) e motori di ricerca, si sono fornite indicazioni specifiche sia sulle modalità per l'esercizio di uno dei diritti più innovativi sanciti dal RGPD, sia sui criteri che possono assistere i titolari (ossia i motori di ricerca) nel rifiutare agli interessati tale diritto. Le linee guida si compongono infatti di due parti: la prima si sofferma sui presupposti che inducono l'interessato ad effettuare una richiesta di deindicizzazione; la seconda, invece, esamina il regime di eccezioni, che consentono al titolare del trattamento di non adempiere alla richiesta dell'interessato. L'art. 17 del RGPD riconosce all'interessato il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano, senza ingiustificato ritardo, se sussiste almeno uno dei sei motivi elencati

dalla lett. a) alla lett. f) del suo paragrafo 1; l'EDPB li esamina tutti e di ciascuno offre un'interpretazione orientata all'esperienza raccolta e alla giurisprudenza (per esempio in tema di necessità del trattamento, di contemperamento con altri diritti del titolare in caso di opposizione al trattamento da parte dell'interessato, o rispetto alla nozione di illiceità del trattamento, e così via). Quanto alle ipotesi in cui l'esercizio del diritto all'oblio può essere rifiutato dal titolare, le linee guida si soffermano sul possibile contrasto fra cancellazione e "libertà di espressione" alla luce della giurisprudenza Ue e CEDU nonché sulla possibile esistenza di obblighi di pubblicazione sanciti per legge, e sottolineano come il motore di ricerca debba essere in grado di dimostrare che la cancellazione di un determinato contenuto della pagina dei risultati rappresenta un grave ostacolo o impedisce del tutto il raggiungimento delle finalità di archiviazione nell'interesse pubblico, ricerca scientifica o storica o per scopi statistici.

Torna a **Indice** | **Premessa**

Linee guida 5/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca, ai sensi del RGPD (parte 1) - Versione 2.0

Adottate il 7 luglio 2020

Cronologia delle versioni

Versione 2.0	7 luglio 2020	Adozione delle Linee guida dopo la consultazione pubblica
Versione 1.1	17 febbraio 2020	Correzioni minori
Versione 1.0	2 dicembre 2019	Adozione delle Linee guida per consultazione pubblica

Indice

Introduzione

1. Basi giuridiche di una richiesta di deindicizzazione ai sensi del RGPD
   - 1.1 Motivazione 1: il diritto di chiedere la deindicizzazione quando i dati personali non sono più necessari rispetto al trattamento del fornitore del motore di ricerca (articolo 17, paragrafo 1, lettera a))
   - 1.2 Motivazione 2: il diritto di chiedere la deindecizzazione quando l'interessato revoca il consenso nel caso in cui il fondamento giuridico del trattamento sia conforme all'articolo 6, paragrafo 1, lettera a)
   - 1.3 Motivazione 3: il diritto di chiedere la deindicizzazione quando l'interessato ha esercitato il diritto di opporsi al trattamento dei suoi dati personali (articolo 17, paragrafo 1, lettera b))
   - 1.4 Motivazione 4: il diritto di chiedere la deindicizzazione quando i dati personali sono stati trattati illecitamente (articolo 17, paragrafo 1, lettera d))
   - 1.5 Motivazione 5: il diritto di chiedere la deindicizzazione quando i dati personali sono stati cancellati per adempiere un obbligo legale (articolo 17, paragrafo 1, lettera e))
   - 1.6 Motivazione 6: il diritto di chiedere la deindicizzazione quando i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione a minori (articolo 17, paragrafo 1, lettera f))

2. Le eccezioni al diritto di chiedere la deindicizzazione ai sensi dell'articolo 17, paragrafo 3
   - 2.1 Il trattamento è necessario per l'esercizio del diritto alla libertà di espressione e di informazione
   - 2.2 Il trattamento è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento
     - 2.2.1 Obbligo legale
     - 2.2.2 Esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri
   - 2.3 Motivi di interesse pubblico nel settore della sanità pubblica
   - 2.4 Finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o finalità statistiche conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento
   - 2.5 Accertamento, esercizio o difesa di un diritto in sede giudiziaria

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in appresso «RGPD»), visto l'accordo SEE, in particolare l'allegato XI e il protocollo n. 37 dello stesso, modificati dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

visti l'articolo 12 e l'articolo 22 del regolamento interno,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

INTRODUZIONE

1. In esito alla sentenza Costeja della Corte di giustizia dell'Unione europea («**CGUE**») del 13 maggio 2014[2], un interessato può richiedere al fornitore di un motore di ricerca online («**fornitore del motore di ricerca**»)[3], di cancellare uno o più link verso pagine web dall'elenco di risultati che appare dopo una ricerca effettuata a partire dal suo nome.
2. Secondo la relazione sulla trasparenza di Google[4], la percentuale di URL che Google non ha rimosso dall'elenco non è aumentata nel corso degli ultimi 5 anni dopo l'emanazione di detta sentenza. Tuttavia, successivamente alla sentenza della CGUE, gli interessati sembrano essere più consapevoli del loro diritto di presentare un reclamo avverso il rifiuto delle loro richieste di deindicizzazione, considerato che le autorità di controllo hanno osservato un aumento del numero di reclami riguardanti il rifiuto da parte dei fornitori di motori di ricerca di deindicizzare link.
3. Il comitato europeo per la protezione dei dati («**comitato**»), conformemente al proprio piano d'azione, sta sviluppando linee guida in merito all'articolo 17 del regolamento generale sulla protezione dei dati («**RGPD**»). Fino a quando tali linee guida non saranno ultimate, le autorità di controllo devono continuare a gestire e a svolgere indagini sui reclami presentati dagli interessati nella misura del possibile e in maniera ragionevolmente tempestiva.
4. Pertanto, il presente documento intende fornire un'interpretazione del diritto all'oblio nei casi dei motori di ricerca alla luce delle disposizioni dell'articolo 17 del RGPD (il «diritto di richiedere la deindicizzazione»). Difatti, il diritto all'oblio è stato introdotto, in particolare, nel quadro dell'articolo 17 del RGPD per tenere conto del diritto di richiedere la deindicizzazione stabilito dalla sentenza Costeja.
5. Tuttavia, come previsto dalla direttiva 95/46/CE del 24 ottobre 1995 (la «**direttiva**») e come statuito dalla CGUE nella succitata sentenza Costeja[5], il diritto di richiedere la deindicizzazione implica due diritti (il diritto di opposizione e il diritto alla cancellazione RGPD). L'applicazione dell'articolo 21 è infatti espressamente prevista quale terzo motivo per esercitare il diritto alla cancellazione. Pertanto, sia l'articolo 17 sia l'articolo 21 del RGPD possono fungere da fondamento giuridico per le richieste di deindicizzazione. Il diritto di opposizione e il diritto di ottenere la cancellazione erano già stati riconosciuti dalla direttiva. Tuttavia, come vedremo, la formulazione del RGPD richiede un adeguamento dell'interpretazione di tali diritti.
6. A titolo preliminare occorre osservare che, mentre l'articolo 17 del RGPD è applicabile a tutti i titolari del trattamento, il presente documento si concentra esclusivamente sul trattamento da parte dei fornitori di motori di ricerca e sulle richieste di deindicizzazione presentate dagli interessati.
7. Occorre svolgere alcune considerazioni per quanto concerne l'applicazione dell'articolo 17 del RGPD in rapporto al trattamento dei dati da parte di un fornitore di motore di ricerca. A tal proposito, è necessario precisare che il trattamento dei dati personali effettuato nel quadro dell'attività del fornitore

di un motore di ricerca deve essere distinto dal trattamento operato degli editori dei siti web di terzi (come i mezzi di comunicazione) che forniscono contenuti giornalistici online[6].

8. Se un interessato ottiene la deindicizzazione di un particolare contenuto, ciò determina la cancellazione di tale contenuto specifico dall'elenco dei risultati di ricerca relativi all'interessato, quando la ricerca è, in via generale, effettuata a partire dal suo nome. Il contenuto resterà tuttavia disponibile se vengono utilizzati altri criteri di ricerca.

9. Le richieste di deindicizzazione non comportano la cancellazione completa dei dati personali. Infatti, i dati personali non saranno cancellati né dal sito web di origine né dall'indice e dalla cache del fornitore del motore di ricerca. Ad esempio, un interessato può richiedere la rimozione dall'indice di un motore di ricerca di dati personali provenienti da un mezzo di comunicazione, quale un articolo di giornale. In questo caso, il link ai dati personali può essere rimosso dall'indice del motore di ricerca, ma l'articolo in questione resterà comunque sotto il controllo del mezzo di comunicazione e può rimanere pubblicamente disponibile e accessibile, sebbene non sia più visibile nei risultati di ricerca basati sulle interrogazioni che includono, in linea di principio, il nome dell'interessato.

10. Tuttavia, i fornitori di motori di ricerca non sono esonerati, in via generale, dall'obbligo di cancellazione completa. In alcuni casi eccezionali, dovranno effettuare la cancellazione effettiva e completa dei propri indici o cache. Ad esempio, nei casi in cui i fornitori di motori di ricerca non rispettassero più le richieste robots.txt attuate dall'editore originario, avrebbero effettivamente l'obbligo di cancellare completamente l'URL corrispondente al contenuto, a differenza della deindicizzazione che è principalmente basata sul nome dell'interessato.

11. Il presente documento affronta due temi. Il primo tema riguarda i motivi che un interessato può invocare per chiedere la deindicizzazione a un fornitore di motore di ricerca ai sensi dell'articolo 17, paragrafo 1, del RGPD. Il secondo riguarda le eccezioni al diritto di richiedere la deindicizzazione ai sensi dell'articolo 17, paragrafo 3, del RGPD. Il presente documento sarà integrato da un allegato dedicato alla valutazione dei criteri per gestire i reclami relativi al diniego di un richiesta di deindicizzazione.

12. Il presente documento non tratta dell'articolo 17, paragrafo 2[7], del RGPD. Tale articolo impone infatti ai titolari del trattamento che hanno reso pubblici dati personali di informare i titolari che hanno successivamente riutilizzato tali dati personali mediante link, copia o riproduzione. Tale obbligo di informazione non si applica ai fornitori di motori di ricerca quando trovano informazioni contenenti dati personali pubblicate o rese disponibili su Internet da terzi, le indicizzano in maniera automatica, le memorizzano temporaneamente e infine le mettono a disposizione degli utenti di Internet secondo un determinato ordine di preferenza[8]. Inoltre, l'articolo non impone ai fornitori di motori di ricerca, che hanno ricevuto una richiesta di deindicizzazione da parte di un interessato, di informare il terzo che ha reso pubblica tale infor-

mazione su Internet. Questo obbligo intende rafforzare la responsabilità dei titolari originari del trattamento e impedire il moltiplicarsi delle iniziative assunte dagli interessati. A tal proposito, rimane valido quanto affermato dal gruppo "Articolo 29", ossia che i fornitori di motori di ricerca «*non dovrebbero, quale prassi generale, informare i webmaster delle pagine deindicizzate del fatto che non si riesca ad accedere ad alcune pagine web dal motore di ricerca in risposta ad una specifica interrogazione» in quanto «non esiste alcun fondamento giuridico per una tale comunicazione ai sensi della normativa UE sulla protezione dei dati*»[9]. Si prevede di sviluppare linee guida specifiche e distinte anche in merito all'articolo 17, paragrafo 2, del RGPD.

1. BASI GIURIDICHE DI UNA RICHIESTA DI DEINDICIZZAZIONE AI SENSI DEL RGPD

13. Il diritto di richiedere la deindicizzazione previsto dall'articolo 17 del RGPD non inficia le conclusioni della sentenza Costeja, in cui la CGUE ha statuito che una richiesta di deindicizzazione trovava fondamento nel diritto di rettifica/cancellazione e nel diritto di opposizione ai sensi, rispettivamente, degli articoli 12 e 14 della direttiva.

14. L'articolo 17, paragrafo 1, stabilisce un principio generale per cancellare i dati nei sei casi seguenti:
    a. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati *(articolo 17, paragrafo 1, lettera a)*;
    b. l'interessato revoca il consenso su cui si basa il trattamento *(articolo 17, paragrafo 1, lettera b)*;
    c. l'interessato esercita il diritto di opporsi al trattamento dei suoi dati personali ai sensi dell'articolo 21, paragrafi 1 e 2, del RGPD;
    d. i dati personali sono stati trattati illecitamente *(articolo 17, paragrafo 1, lettera d)*;
    e. la cancellazione adempie un obbligo legale *(articolo 17, paragrafo 1, lettera e)*;
    f. i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione a minori *(articolo 17, paragrafo 1, lettera f), che rinvia all'articolo 8, paragrafo 1)*.

15. Sebbene tutti i motivi di cui all'articolo 17 siano teoricamente applicabili quando si tratta di procedere a una deindicizzazione, in pratica alcuni non verranno mai utilizzati o lo saranno solo raramente, come nel caso della revoca del consenso (cfr. motivo 2 di seguito).

16. Un interessato potrebbe tuttavia presentare una richiesta di deindicizzazione a un fornitore di motori di ricerca sulla base di uno o più motivi. Ad esempio, un interessato potrebbe richiedere la deindicizzazione perché non ritiene più necessario che i suoi dati personali siano trattati dal motore di ricerca (articolo 17, paragrafo 1, lettera a)) ed esercitare anche il diritto di opporsi al trattamento ai sensi dell'articolo 21, paragrafo 1, del RGPD (articolo 17, paragrafo 1, lettera c)).

17. Onde valutare i reclami riguardanti un fornitore di motori di ricerca che si è

rifiutato di cancellare un particolare risultato di ricerca ai sensi dell'articolo 17 del RGPD, le autorità di controllo dovrebbero stabilire se il contenuto cui si riferisce un URL debba essere deindicizzato o meno. Nell'analizzare il merito del reclamo, le autorità dovrebbero quindi tenere conto della natura del contenuto reso disponibile dagli editori dei siti web terzi.

1.1 MOTIVAZIONE 1: IL DIRITTO DI CHIEDERE LA DEINDICIZZAZIONE QUANDO I DATI PERSONALI NON SONO PIÙ NECESSARI RISPETTO AL TRATTAMENTO DEL FORNITORE DEL MOTORE DI RICERCA (ARTICOLO 17, PARAGRAFO 1, LETTERA A))

18. Ai sensi dell'articolo 17, paragrafo 1, lettera a), del RGPD, un interessato può richiedere a un fornitore di motore di ricerca, a seguito di una ricerca effettuata in via generale a partire dal suo nome, di rimuovere contenuti dall'elenco dei risultati di ricerca, qualora i dati personali dell'interessato apparsi in questi risultati di ricerca non siano più necessari rispetto alle finalità del trattamento del motore di ricerca.
19. Questa disposizione consente a un interessato di chiedere la deindicizzazione delle informazioni personali che lo riguardano rese accessibili per un periodo superiore a quello necessario per il trattamento ad opera del fornitore del motore di ricerca. Tuttavia, tale trattamento è effettuato in particolare per rendere le informazioni più facilmente accessibili agli utenti di Internet. Nell'ambito del diritto di chiedere la deindicizzazione, deve essere raggiunto un equilibrio tra la tutela della vita privata e gli interessi degli utenti di Internet ad avere accesso all'informazione. In particolare, occorre valutare se con il passare del tempo i dati personali siano diventati obsoleti o non siano stati aggiornati.
20. Ad esempio, un interessato può esercitare il diritto di chiedere la deindicizzazione ai sensi dell'articolo 17, paragrafo 1, lettera a), quando:

- le informazioni che lo riguardano detenute da un'impresa sono state eliminate dal registro pubblico;
- un link a un sito web di un'azienda contiene i suoi dati di contatto sebbene non lavori più per quell'azienda;
- è necessario pubblicare informazioni su Internet per diversi anni in adempimento di un obbligo legale e queste sono rimaste online per un periodo di tempo superiore a quanto specificato dalla legislazione.

21. Come dimostrato dagli esempi, un interessato può chiedere in particolare la deindicizzazione di un determinato contenuto, laddove le informazioni personali siano chiaramente inesatte perché obsolete o datate. Una tale valutazione dipenderà, tra l'altro, dalle finalità del trattamento originario. Di conseguenza, le autorità di controllo dovrebbero anche tenere conto dei periodi di conservazione iniziali dei dati personali, ove disponibili, allorché effettuano la loro analisi in merito alle richieste di deindicizzazione ai sensi dell'articolo 17, paragrafo 1, lettera a), del RGPD.

1.2 MOTIVAZIONE 2: IL DIRITTO DI CHIEDERE LA DEINDICIZZAZIONE QUANDO L'INTERESSATO REVOCA IL CONSENSO NEL CASO IN CUI IL FONDAMENTO GIURIDICO DEL TRATTAMENTO SIA CONFORME ALL'ARTICOLO 6, PARAGRAFO 1, LETTERA A), O ALL'ARTICOLO 9, PARAGRAFO 2, LETTERA A), DEL RGPD E SE NON SUSSISTE ALTRO FONDAMENTO GIURIDICO PER IL TRATTAMENTO (ARTICOLO 17, PARAGRAFO 1, LETTERA B))

22. Ai sensi dell'articolo 17, paragrafo 1, lettera b), del RGPD, un interessato può ottenere la cancellazione dei dati personali che lo riguardano se revoca il consenso al trattamento.
23. In caso di deindicizzazione, ciò significherebbe che il fornitore del motore di ricerca si sarebbe avvalso del consenso dell'interessato quale base legale per il trattamento. L'articolo 17, paragrafo 1, del RGPD solleva infatti la questione della base legale del trattamento utilizzata da un fornitore del motore di ricerca per produrre i risultati del motore di ricerca, tra cui i dati personali.
24. Per tale ragione, sembra improbabile che una richiesta di deindicizzazione sia presentata da un interessato che desideri revocare il consenso perché il titolare del trattamento, a cui ha dato il proprio consenso, è l'editore web e non il gestore del motore di ricerca che indicizza i dati. Questa interpretazione è stata confermata dalla CGUE nella propria sentenza C-136-17 del 24 settembre 2019 (la «**sentenza Google 2**»)[10]. La Corte indica che *«(...) il consenso deve essere "specifico" e vertere quindi specificamente sul trattamento effettuato nell'ambito dell'attività del motore di ricerca (...). Orbene, in pratica è difficilmente ipotizzabile (...) che il gestore di un motore di ricerca chieda il consenso esplicito degli interessati prima di procedere, per le necessità della sua attività di indicizzazione, al trattamento dei dati personali che li riguardano. In ogni caso, (...) il fatto stesso che una persona presenti una richiesta di deindicizzazione significa, in linea di principio, che, quanto meno alla data di tale richiesta, non acconsente più al trattamento effettuato dal gestore del motore di ricerca.»*
25. Ciononostante, se un interessato revocasse il proprio consenso a utilizzare i suoi dati su una particolare pagina web, l'editore originario di tale pagina web dovrebbe informare i fornitori di motori di ricerca che hanno indicizzato i dati ai sensi dell'articolo 17, paragrafo 2, del RGPD. L'interessato avrebbe comunque diritto a ottenere la deindicizzazione dei dati personali che lo riguardano, ma in tal caso ai sensi dell'articolo 17, paragrafo 1, lettera c).

1.3 MOTIVAZIONE 3: IL DIRITTO DI CHIEDERE LA DEINDICIZZAZIONE QUANDO L'INTERESSATO HA ESERCITATO IL DIRITTO DI OPPORSI AL TRATTAMENTO DEI SUOI DATI PERSONALI (ARTICOLO 17, PARAGRAFO 1, LETTERA C))

26. Ai sensi dell'articolo 17, paragrafo 1, lettera c) del RGPD, un interessato può ottenere la cancellazione dei dati personali che lo riguardano dal fornitore del motore di ricerca, laddove l'interessato si opponga al trattamento ai sensi dell'articolo 21, paragrafo 1, del RGPD e non sussiste alcun motivo legittimo prevalente per procedere al trattamento ad opera del titolare.

27. Il diritto di opposizione offre agli interessati maggiori garanzie, poiché non limita i motivi in base ai quali gli interessati possono chiedere la deindicizzazione come invece avviene nel caso dell'articolo 17, paragrafo 1, del RGPD.

28. Il diritto di opporsi al trattamento è stato previsto dall'articolo 14 della direttiva[11] e ha costituito un fondamento giuridico delle richieste di deindicizzazione sin dalla sentenza Costeja. Tuttavia, le differenze nella formulazione dell'articolo 21 del RGPD e dell'articolo 14 della direttiva indicano che vi possono essere anche differenze nella rispettiva applicazione.

29. Ai sensi della direttiva, l'interessato doveva basare la propria richiesta su «*motivi preminenti e legittimi, derivanti dalla sua situazione particolare». Quanto al RGPD, un interessato può opporsi al trattamento «per motivi connessi alla sua situazione particolare*». Pertanto, questi non deve più dimostrare l'esistenza di «*motivi preminenti e legittimi*».

30. Il RGPD modifica pertanto l'onere della prova, stabilendo una presunzione a favore dell'interessato e obbligando, al contrario, il titolare del trattamento a dimostrare l'esistenza di «*motivi legittimi cogenti per procedere al trattamento*» (articolo 21, paragrafo 1). Pertanto, quando un fornitore di motore di ricerca riceve una richiesta di deindicizzazione fondata sulla situazione particolare dell'interessato, è tenuto ora a cancellare i dati personali ai sensi dell'articolo 17, paragrafo 1, lettera c), del RGPD, a meno che possa dimostrare che sussiste un «*motivo legittimo prevalente*» per l'inclusione in un elenco dello specifico risultato di ricerca che, in combinato disposto con l'articolo 21, paragrafo 1, configuri «*motivi legittimi cogenti (...) che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato*». Il fornitore del motore di ricerca può stabilire se sussiste un «*motivo legittimo prevalente*», inclusa qualsiasi esenzione prevista dall'articolo 17, paragrafo 3, del RGPD. Tuttavia, se il fornitore del motore di ricerca non dimostra l'esistenza di un motivo legittimo prevalente, l'interessato ha il diritto di ottenere la deindicizzazione ai sensi dell'articolo 17, paragrafo 1, lettera c), del RGPD. Di fatto, le richieste di deindicizzazione comportano ora la necessità di un bilanciamento tra le ragioni riguardanti la situazione particolare dell'interessato e i motivi legittimi e cogenti del fornitore del motore di ricerca. Il bilanciamento tra la tutela della vita privata e gli interessi degli utenti di Internet ad avere accesso all'informazione come stabilito dalla CGUE nella sentenza Costeja può essere pertinente ai fini di questa valutazione, così come quello realizzato dalla Corte europea dei diritti dell'uomo (Corte EDU) nelle sentenze relative alla libertà di informazione.

31. Pertanto, i criteri di deindicizzazione definiti dal gruppo "Articolo 29" nelle linee guida sull'attuazione della sentenza della Corte di giustizia dell'Unione nella causa C-131/12 «Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González» possono ancora essere utilizzati dai fornitori di motori di ricerca e dalle autorità di controllo per valutare una richiesta di deindicizzazione fondata sul diritto di opposizione (articolo 17, paragrafo 1, lettera c), del RGPD).

32. A tal proposito, la richiesta di deindicizzazione si fonderà sulla «*situazione particolare*» dell'interessato (ad esempio, la circostanza per cui un risultato

di ricerca arreca danno a un interessato nella ricerca di un impiego o mina la sua reputazione nella vita personale) che sarà presa in considerazione nello stabilire il bilanciamento tra i diritti personali e il diritto all'informazione, in aggiunta ai criteri classici per gestire le richieste di deindicizzazione, quali:

- l'interessato non è una figura pubblica;
- le informazioni in questione non sono attinenti alla vita professionale dell'interessato, ma si ripercuotono sulla sua vita privata;
- le informazioni costituiscono incitamento all'odio, calunnia, diffamazione o analoghi reati di opinione contro l'interessato come sancito da una decisione giudiziale;
- i dati sembrano verificati, ma sono di fatto inesatti;
- le informazioni si riferiscono a un reato di gravità relativamente minore commesso molto tempo prima e arrecano pregiudizio all'interessato.

33. Tuttavia, tali criteri non dovranno essere esaminati in assenza di elementi che comprovino la sussistenza di motivi legittimi e cogenti per rifiutare la richiesta.

1.4 MOTIVAZIONE 4: IL DIRITTO DI CHIEDERE LA DEINDICIZZAZIONE QUANDO I DATI PERSONALI SONO STATI TRATTATI ILLECITAMENTE (ARTICOLO 17, PARAGRAFO 1, LETTERA D))

34. Ai sensi dell'articolo 17, paragrafo 1, lettera d), del RGPD, un interessato può ottenere la cancellazione dei dati personali che lo riguardano nel caso in cui questi siano stati trattati illecitamente.

35. Il concetto di trattamento illecito va innanzitutto interpretato alla luce dell'articolo 6 del RGPD sulla liceità del trattamento. Gli altri principi stabiliti dal RGPD (come i principi dell'articolo 5 del RGPD o di altre disposizioni del capo II) possono contribuire a tale interpretazione.

36. Questo concetto va, in secondo luogo, interpretato estensivamente quale violazione di una disposizione di legge diversa dal RGPD. Tale interpretazione deve basarsi su elementi oggettivi alla luce del diritto o della giurisprudenza nazionali. Ad esempio, una richiesta di deindicizzazione è accolta laddove l'indicizzazione è stata vietata espressamente da un'ordinanza del tribunale.

    Qualora un fornitore di motore di ricerca non sia in grado di dimostrare l'esistenza di un fondamento giuridico per il trattamento, una richiesta di deindicizzazione può rientrare nell'ambito di applicazione dell'articolo 17, paragrafo 1, lettera d), del RGPD, poiché il trattamento dei dati personali in questi casi deve essere considerato illecito. Tuttavia, occorre ricordare che nel caso di illiceità del trattamento originario, l'interessato ha comunque il diritto di chiedere la deindicizzazione ai sensi dell'articolo 17, paragrafo 1, lettera c), del RGPD.

1.5 MOTIVAZIONE 5: IL DIRITTO DI CHIEDERE LA DEINDICIZZAZIONE QUANDO I DATI PERSONALI SONO STATI CANCELLATI PER ADEMPIERE UN OBBLIGO LEGALE (ARTICOLO 17, PARAGRAFO 1, LETTERA E))

37. Ai sensi dell'articolo 17, paragrafo 1, lettera e), del RGPD, un interessato può chiedere al fornitore del motore di ricerca di deindicizzare uno o più risultati di ricerca, se i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il fornitore del motore di ricerca.

38. La necessità di adempiere un obbligo legale può derivare da un'ingiunzione, da una espressa previsione del diritto interno o dell'Unione in quanto sussiste un «obbligo legale alla cancellazione» o dalla semplice violazione del periodo di conservazione da parte del fornitore del motore di ricerca. Un esempio potrebbe essere rappresentato dalla non osservanza del periodo di conservazione fissato per legge (anche se questa ipotesi riguarda principalmente i documenti pubblici). In un caso del genere potrebbero ricadere anche dati non anonimizzati o identificativi messi a disposizione come dati aperti.

1.6 MOTIVAZIONE 6: IL DIRITTO DI CHIEDERE LA DEINDICIZZAZIONE QUANDO I DATI PERSONALI SONO STATI RACCOLTI RELATIVAMENTE ALL'OFFERTA DI SERVIZI DELLA SOCIETÀ DELL'INFORMAZIONE A MINORI (ARTICOLO 17, PARAGRAFO 1, LETTERA F))

39. Ai sensi dell'articolo 17, paragrafo 1, lettera f), del RGPD, un interessato può chiedere a un fornitore del motore di ricerca di deindicizzare uno o più risultati se i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione a minori, nei termini di cui all'articolo 8, paragrafo 1, del RGPD.

40. L'articolo riguarda l'offerta diretta di servizi della società dell'informazione e nessun altro tipo di trattamento. Il RGPD non definisce i servizi della società dell'informazione, ma rimanda alle definizioni esistenti nel diritto dell'UE[12]. Vi sono difficoltà nell'interpretazione in quanto il considerando 18 della direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, fornisce una definizione ampia e ambigua del concetto di «*offerta diretta di servizi della società dell'informazione».* Essa indica soprattutto che questi servizi *«abbracciano una vasta gamma di attività economiche svolte in linea (on line)*», ma specifica che non si tratta esclusivamente di «*servizi che portano a stipulare contratti in linea ma anche di servizi non remunerati dal loro destinatario, **nella misura in cui costituiscono un'attività economica**, come l'offerta di informazioni o comunicazioni commerciali in linea o la fornitura di strumenti per la ricerca, l'accesso e il reperimento di dati*», definendo poi i criteri di un'attività economica.

41. Da quanto precede si desume che le attività dei fornitori di motori di ricerca rientrano probabilmente nell'ambito di applicazione dell'offerta diret-

ta di servizi della società dell'informazione. Tuttavia, i fornitori di motori di ricerca non verificano se i dati personali che indicizzano riguardino o meno un minore. Alla luce delle loro specifiche responsabilità e fatta salva l'applicazione dell'articolo 17, paragrafo 3, del RGPD, essi dovrebbero però deindicizzare un contenuto riguardante un minore ai sensi dell'articolo 17, paragrafo 1, lettera c), del RGPD, riconoscendo che il fatto di essere un minore è un valido «motivo connesso ad una situazione particolare» (articolo 21 del RGPD) e che «*i minori meritano una specifica protezione relativamente ai loro dati personali*»" (considerando 38 del RGPD). In tal caso, deve essere preso in considerazione l'ambito della raccolta dei dati personali da parte del titolare del trattamento. In particolare, si deve tenere conto della data di inizio del trattamento da parte del sito web originario quando un interessato chiede la deindicizzazione dello specifico contenuto.

2. LE ECCEZIONI AL DIRITTO DI CHIEDERE LA DEINDICIZZAZIONE AI SENSI DELL'ARTICOLO 17, PARAGRAFO 3

42. L'articolo 17, paragrafo 3, del RGPD afferma che i paragrafi 1 e 2 dell'articolo 17 del RGPD non si applicheranno quando il trattamento è necessario:
    a. per l'esercizio del diritto alla libertà di espressione e di informazione *(articolo 17, paragrafo 3, lettera a))*;
    b. per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento *(articolo 17, paragrafo 3, lettera b))*;
    c. per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3 *(articolo 17, paragrafo 3, lettera c))*;
    d. a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento *(articolo 17, paragrafo 3, lettera d))*; o
    e. per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria *(articolo 17, paragrafo 3, lettera e))*.

43. Questa sezione intende dimostrare che la maggior parte delle eccezioni di cui all'articolo 17, paragrafo 3, del RGPD non sembrano attagliarsi alle richieste di deindicizzazione. Tale inadeguatezza depone a favore dell'applicazione dell'articolo 21 del RGPD per le richieste di deindicizzazione. In ogni caso, occorre ricordare che le eccezioni di cui all'articolo 17, paragrafo 3, del RGPD possono essere invocate quali motivi legittimi prevalenti ai sensi dell'articolo 17, paragrafo 1, lettera c), del RGPD.

2.1 IL TRATTAMENTO È NECESSARIO PER L'ESERCIZIO DEL DIRITTO ALLA LIBERTÀ DI ESPRESSIONE E DI INFORMAZIONE

44. Questa eccezione all'applicazione dell'articolo 17, paragrafo 1, del RGPD deve essere interpretata e applicata nell'ambito delle caratteristiche che definiscono la cancellazione. L'articolo 17, paragrafo 1, del RGPD è formulato nei termini di un mandato chiaro e incondizionato rivolto ai titolari del trattamento. Se le condizioni stabilite nell'articolo 17, paragrafo 1, del RGPD, sono soddisfatte, il titolare del trattamento «*ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali*». Tuttavia, non si tratta di un diritto assoluto. Le eccezioni di cui all'articolo 17, paragrafo 3, del RGPD, individuano i casi in cui questo obbligo non si applica.

45. Tuttavia, l'equilibrio tra la tutela dei diritti delle parti interessate e la libertà di espressione, incluso il libero accesso alle informazioni, costituisce parte integrante dell'articolo 17 del RGPD.

46. La CGUE ha riconosciuto nella sentenza Costeja, e lo ha ripetuto di recente nella sentenza Google 2, che il trattamento effettuato da un fornitore di motore di ricerca può incidere significativamente sui diritti fondamentali alla vita privata e alla protezione dei dati quando la ricerca è effettuata utilizzando il nome di un interessato.

47. Nel valutare i diritti e le libertà degli interessati e gli interessi degli utenti di Internet ad avere accesso all'informazione tramite il fornitore del motore di ricerca, la Corte ha fornito la seguente interpretazione: «*Se indubbiamente i diritti della persona interessata tutelati da tali articoli prevalgono, di norma, anche sul citato interesse degli utenti di Internet, tale equilibrio può nondimeno dipendere, in casi particolari, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica.*»[13]

48. La Corte ha altresì ritenuto che i diritti degli interessati prevarranno, in linea generale[14], sull'interesse degli utenti di Internet ad avere accesso all'informazione tramite il fornitore del motore di ricerca. Tuttavia, ha individuato diversi fattori che possono influenzare tale determinazione. Tra di essi figurano: la natura dell'informazione o il suo carattere sensibile, in particolare l'interesse degli utenti di Internet ad avere accesso all'informazione, il quale può variare a seconda del ruolo che tale persona interessata riveste nella vita pubblica.

49. L'analisi svolta dalla Corte in tema di deindicizzazione implica che, nel valutare le richieste di deindicizzazione, la decisione sul mantenimento o il blocco dei risultati di ricerca da parte del fornitore del motore di ricerca debba necessariamente valutare quale sarebbe l'impatto di una decisione di deindicizzazione sull'accesso alle informazioni da parte degli utenti di Internet[15]. Tale impatto non comporta per forza di cose il rigetto di una richiesta di deindicizzazione. Come confermato dalla Corte, una tale interferenza con i diritti fondamentali dell'interessato deve essere giustificata dall'interesse preponderante del pubblico ad avere accesso all'informazione.

50. La Corte ha altresì distinto tra la legittimità della diffusione di informazioni da parte dell'editore di un sito web e la legittimità di tale diffusione da parte del fornitore del motore di ricerca. La Corte ha riconosciuto che l'attività di un editore web può perseguire esclusivamente i fini giornalistici, nel qual caso l'editore web beneficerebbe delle esenzioni che gli Stati membri possono stabilire in questi casi sulla base dell'articolo 9 della direttiva (attualmente articolo 85, paragrafo 2, del RGPD). A tal proposito, nella sentenza «*M.L. e W.W. contro Germania*», del 28 giugno 2018, la Corte EDU indica che l'equilibrio degli interessi in gioco può produrre risultati diversi in base alla specifica richiesta – distinguendo tra i) una richiesta di cancellazione rivolta all'editore originario, la cui attività è il nucleo essenziale di ciò che mira a tutelare la libertà di espressione e ii) una richiesta nei confronti del motore di ricerca, il cui primo interesse non è quello di pubblicare le informazioni originarie sull'interessato, ma consentire in particolare l'identificazione delle informazioni disponibili su tale persona e dunque stabilire il suo profilo.

51. Queste considerazioni dovrebbero trovare applicazione in relazione ai reclami concernenti l'articolo 17 del RGPD, dal momento che nelle decisioni in materia i diritti degli interessati che hanno chiesto la deindicizzazione devono essere valutati alla luce degli interessi degli utenti di Internet ad avere accesso all'informazione.

52. Come chiarito dalla CGUE nella sentenza Google 2, l'articolo 17, paragrafo 3, lettera a), del RGPD è «*espressione del fatto che il diritto alla protezione dei dati personali non è un diritto assoluto, ma deve (...) essere considerato in relazione alla sua funzione sociale ed essere bilanciato con altri diritti fondamentali, conformemente al principio di proporzionalità*»[16]. Esso «p*revede quindi espressamente il requisito del bilanciamento tra, da un lato, i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, sanciti agli articoli 7 e 8 della Carta e, d'altro lato, il diritto fondamentale alla libertà di informazione, garantito dall'articolo 11 della Carta.*»[17]

53. La Corte conclude che «*il gestore di un motore di ricerca, quando riceve una richiesta di deindicizzazione riguardante un link verso una pagina web nella quale sono pubblicati dati personali rientranti nelle categorie particolari (...), deve – sulla base di tutti gli elementi pertinenti della fattispecie e tenuto conto della gravità dell'ingerenza nei diritti fondamentali della persona interessata al rispetto della vita privata e alla protezione dei dati personali, sanciti dagli articoli 7 e 8 della Carta – verificare, alla luce dei motivi di interesse pubblico rilevante (...), se l'inserimento di detto link nell'elenco dei risultati, visualizzato in esito ad una ricerca effettuata a partire dal nome della persona in questione, si riveli strettamente necessario per proteggere la libertà di informazione degli utenti di Internet potenzialmente interessati ad avere accesso a tale pagina web mediante una ricerca siffatta, libertà che è sancita all'articolo 11 della Carta.*»[18]

54. Per concludere, a seconda delle circostanze del caso, i fornitori di motori di ricerca possono rifiutare la deindicizzazione di un contenuto qualora possano dimostrare che l'inserimento di tale contenuto nell'elenco di risultati è strettamente necessario per la tutela della libertà di informazione degli utenti di Internet.

2.2 IL TRATTAMENTO È NECESSARIO PER L'ADEMPIMENTO DI UN OBBLIGO LEGALE CUI È SOGGETTO IL TITOLARE DEL TRATTAMENTO O PER L'ESECUZIONE DI UN COMPITO SVOLTO NEL PUBBLICO INTERESSE OPPURE NELL'ESERCIZIO DI PUBBLICI POTERI DI CUI È INVESTITO IL TITOLARE DEL TRATTAMENTO

55. Il contenuto di questa eccezione è difficilmente applicabile all'attività dei fornitori di motori di ricerca e può influire sulle decisioni di deindicizzare alcuni risultati, poiché il trattamento dei dati da parte dei fornitori di motori di ricerca si basa, in linea di principio, sul loro legittimo interesse.

2.2.1. OBBLIGO LEGALE

56. È difficile immaginare l'esistenza di disposizioni di legge che obblighino i fornitori di motori di ricerca a divulgare determinate informazioni. Tale circostanza deriva dal tipo di attività svolta dai fornitori in questione, i quali non producono né presentano informazioni.

57. Pertanto, si ritiene improbabile che il diritto di uno Stato membro preveda l'obbligo per i fornitori di motori di ricerca di pubblicare determinati tipi di informazione, anziché stabilire che l'obbligo di procedere a tale pubblicazione debba essere assolto da altre pagine web che saranno poi collegate dai fornitori di motori di ricerca.

58. Analoghe considerazioni valgono quanto alla possibilità che il diritto dell'Unione o dello Stato membro consenta a un'autorità pubblica di prendere decisioni che obblighino i fornitori di motori di ricerca a pubblicare informazioni direttamente anziché mediante i link URL alla pagina web dove sono contenute le informazioni.

59. Qualora il diritto di uno Stato membro stabilisca l'obbligo per i fornitori di motori di ricerca di pubblicare decisioni o documenti contenenti informazioni personali, o autorizzi le autorità pubbliche a esigere tale pubblicazione, si dovrebbe applicare l'eccezione di cui all'articolo 17, paragrafo 3, lettera b), del RGPD.

60. Nell'applicare l'eccezione suddetta occorre tenere conto dei termini in cui è stabilita, ovvero del fatto che il mantenimento dell'informazione in questione è necessario per ottemperare all'obbligo legale di pubblicazione. Ad esempio, il fatto che un obbligo legale o la decisione assunta da un'autorità a ciò legittimata possa prevedere un termine per la pubblicazione o finalità espressamente dichiarate che possano essere conseguite entro un determinato periodo di tempo. In questi casi, se la richiesta di deindicizzazione è presentata oltre i rispettivi termini, si dovrebbe ritenere che l'eccezione non sia più applicabile.

61. Al contrario, accade di frequente che il diritto di uno Stato membro preveda la pubblicazione su pagine web di informazioni contenenti dati personali. Quest'obbligo legale di pubblicare o mantenere pubblicate determinate in-

formazioni non può essere considerato pertinente ai fini dell'eccezione di cui all'articolo 17, paragrafo 3, lettera b), del RGPD, poiché non è rivolto al fornitore del motore di ricerca, bensì agli editori web i cui contenuti sono posti in connessione dall'indice del fornitore del motore di ricerca. Quest'ultimo non può pertanto invocare l'esistenza dell'obbligo suddetto per rigettare una richiesta di deindicizzazione.

62. Tuttavia, l'obbligo legale di pubblicazione posto in capo agli altri editori web dovrebbe essere tenuto in considerazione quando si effettua il bilanciamento tra i diritti degli interessati e l'interesse degli utenti di Internet ad avere accesso all'informazione. Il fatto che un'informazione debba essere pubblicata online per obblighi di legge o in seguito alla decisione assunta da un'autorità a ciò legittimata è indicativo di un interesse del pubblico ad avere la possibilità di accedere a tale informazione.

63. Questa presunzione dell'esistenza di un interesse prevalente del pubblico non è applicabile negli stessi termini alle pagine web originarie rispetto all'indice dei risultati di un fornitore di motore di ricerca. Sebbene l'obbligo legale di pubblicare informazioni su un determinato sito web possa far concludere che tali informazioni non debbano essere cancellate dalla pagina web, non è detto che sia questa la conclusione relativa ai risultati offerti dal fornitore del motore di ricerca quando il nome di un interessato è utilizzato generalmente quale criterio di ricerca.

64. In casi del genere, la valutazione della richiesta di deindicizzazione non dovrebbe basarsi sull'assunto che l'esistenza di un obbligo legale di pubblicazione implichi necessariamente che, nella misura in cui tale obbligo sia imposto agli editori web originari, il fornitore del motore di ricerca non possa accogliere la richiesta di deindicizzazione.

65. La decisione dovrebbe essere presa, come è la norma, individuando un bilanciamento tra i diritti dell'interessato e l'interesse degli utenti di Internet ad avere accesso a tale informazione tramite il fornitore del motore di ricerca.

2.2.2 ESECUZIONE DI UN COMPITO SVOLTO NEL PUBBLICO INTERESSE OPPURE NELL'ESERCIZIO DI PUBBLICI POTERI

66. I fornitori di motori di ricerca non sono autorità pubbliche e pertanto non esercitano pubblici poteri.

67. Tuttavia, potrebbero esercitare tali poteri se fossero loro attribuiti dal diritto di uno Stato membro o dell'Unione. Analogamente, potrebbero svolgere compiti di pubblico interesse se la loro attività fosse considerata necessaria per soddisfare tale interesse pubblico conformemente alla legislazione nazionale[19].

68. Date le caratteristiche dei fornitori di motori di ricerca, è improbabile che gli Stati membri attribuiscano loro pubblici poteri o considerino la loro attività, o parte di essa, necessaria per il conseguimento di un interesse pubblico riconosciuto dalla legge.

69. Se, a ogni modo, si verifica un caso in cui il diritto degli Stati membri attribuisce ai fornitori di motori di ricerca pubblici poteri o collega la loro attività al perseguimento di un obiettivo di interesse pubblico, essi potrebbero avvalersi dell'eccezione di cui all'articolo 17, paragrafo 3, lettera b), del RGPD. Valgono le considerazioni svolte in precedenza rispetto ai casi in cui il diritto di uno Stato membro preveda in capo ai fornitori di motori di ricerca un obbligo legale di trattare le informazioni in questione.

70. Nel decidere sul rigetto di una richiesta di deindicizzazione per ragioni legate a questa eccezione, occorre determinare se il mantenimento dell'informazione nei risultati del motore di ricerca sia necessario per il conseguimento dell'interesse pubblico perseguito o per l'esercizio dei poteri delegati.

71. D'altro canto, di norma la definizione giuridica di poteri pubblici o di interesse pubblico spetta al singolo Stato membro e se il motore di ricerca rigetta una richiesta di deindicizzazione sulla base dell'eccezione in esame occorre considerare che assume tale decisione poiché ritiene la sua attività necessaria per il conseguimento degli obiettivi di interesse pubblico. Il fornitore del motore di ricerca dovrebbe, in questo caso, fornire le motivazioni per cui ritiene che la sua attività sia svolta nell'interesse pubblico. In assenza di una tale spiegazione, il rifiuto di dare seguito a una richiesta di deindicizzazione presentata dall'interessato non può basarsi sull'eccezione in esame.

72. Ne consegue anche che spetterebbe all'autorità di controllo dello Stato membro di cui si applica la legge trattare un eventuale reclamo, ai sensi dell'articolo 55, paragrafo 2, del RGPD.

2.3 MOTIVI DI INTERESSE PUBBLICO NEL SETTORE DELLA SANITÀ PUBBLICA

73. Questa eccezione configura un caso specifico derivante dalla circostanza che il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico.

74. In questo caso, l'interesse pubblico è limitato al settore della sanità pubblica, ma come per l'interesse pubblico in altri settori, il fondamento di liceità del trattamento deve essere previsto nel diritto dell'Unione o dello Stato membro.

75. Dal punto di vista dell'applicazione di questa eccezione nel contesto dell'attività del fornitore del motore di ricerca, valgono le stesse conclusioni esposte in precedenza. Non sembra probabile che il diritto di uno Stato membro o dell'Unione possa stabilire una relazione tra, da un lato, l'attività del fornitore del motore di ricerca e il mantenimento dell'informazione o di una categoria di informazioni nei risultati del fornitore del motore di ricerca e, dall'altro lato, il conseguimento delle finalità di interesse pubblico nel settore della sanità pubblica.

76. Tale conclusione risulta ancor più evidente se si considera che l'effetto della deindicizzazione consiste soltanto nella rimozione di alcuni risultati dalla pagina dei risultati che viene visualizzata quando si inserisce per lo più un nome quale criterio di ricerca. Ma l'informazione non è cancellata dagli in-

dici dei fornitori di motori di ricerca e può essere estratta utilizzando altri criteri di ricerca.

77. È pertanto difficile immaginare che mantenere questi risultati visibili quando sono effettuate ricerche principalmente a partire dal nome di un interessato possa essere considerato, in linea generale, necessario per motivi di interesse pubblico nel settore della sanità pubblica.

78. I criteri concernenti l'applicabilità delle norme nazionali e l'identificazione delle autorità di controllo competenti a trattare eventuali reclami qualora richieste ai sensi dell'articolo 17 del RGPD siano rigettate sulla base della presente eccezione sono stati discussi in precedenza.

2.4 FINALITÀ DI ARCHIVIAZIONE NEL PUBBLICO INTERESSE, DI RICERCA SCIENTIFICA O STORICA O FINALITÀ STATISTICHE CONFORMEMENTE ALL'ARTICOLO 89, PARAGRAFO 1, NELLA MISURA IN CUI IL DIRITTO DI CUI AL PARAGRAFO 1 RISCHI DI RENDERE IMPOSSIBILE O DI PREGIUDICARE GRAVEMENTE IL CONSEGUIMENTO DEGLI OBIETTIVI DI TALE TRATTAMENTO

79. In questo scenario, il fornitore del motore di ricerca deve essere in grado di dimostrare che la deindicizzazione di un determinato contenuto sulla pagina dei risultati costituisce un serio ostacolo o impedisce totalmente il conseguimento delle finalità di ricerca scientifica o storica o le finalità statistiche.

80. Va inteso che queste finalità devono essere oggettivamente perseguite dal fornitore del motore di ricerca. La possibilità che l'eliminazione dei risultati possa pregiudicare in modo significativo le finalità di ricerca o statistica perseguite dagli utenti del servizio del fornitore del motore di ricerca non è pertinente ai fini dell'applicazione di questa eccezione. Tali finalità, se esistono, dovrebbero essere prese in considerazione nel bilanciamento tra i diritti dell'interessato e gli interessi degli utenti di Internet ad avere accesso all'informazione tramite il fornitore del motore di ricerca.

81. Va inoltre rilevato che queste finalità possono essere oggettivamente perseguite dal fornitore del motore di ricerca senza che sia necessario creare un link, in linea di principio, tra il nome dell'interessato e i risultati di ricerca.

2.5 ACCERTAMENTO, ESERCIZIO O DIFESA DI UN DIRITTO IN SEDE GIUDIZIARIA

82. In linea di massima, è alquanto improbabile che i fornitori di motori di ricerca possano invocare questa eccezione per rigettare richieste di deindicizzazione basate sull'articolo 17 del RGPD.

83. Va inoltre sottolineato che una richiesta di deindicizzazione presuppone l'eliminazione di determinati risultati dalla pagina dei risultati di ricerca mostrata dal fornitore quando il criterio di tale ricerca è sostanzialmente il nome di un interessato. L'informazione resta accessibile utilizzando altri criteri di ricerca.

NOTE

[1] Nelle presenti linee guida, i riferimenti agli «Stati membri» sono da intendersi come riferimenti agli «Stati membri del SEE».

[2] CGUE, causa C 131/12, Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, sentenza del 13 maggio 2014.

[3] Inclusi gli archivi web come archive.org

[4] https://transparencyreport.google.com/eu-privacy/overview?hl=it

[5] CGUE, causa C 131/12, sentenza del 13 maggio 2014, punto 88: «*gli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 devono essere interpretati nel senso che, al fine di rispettare i diritti previsti da tali disposizioni, e sempre che le condizioni da queste fissate siano effettivamente soddisfatte, il gestore di un motore di ricerca è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita*».

[6] CGUE, causa C-131/12, sentenza del 13 maggio 2014; Corte europea dei diritti dell'uomo (Corte EDU), «M.L. e W.W. contro Germania», 28 giugno 2018.

[7] Regolamento 2016/679 (RGPD), articolo 17, paragrafo 2: «*Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.*»

[8] Cfr. CGUE, causa C 136/17, GC e altri contro CNIL, sentenza del 24 settembre 2019, punto 35 e causa C-131/12, sentenza del 13 maggio 2014, punto 41.

[9] Gruppo dell'articolo 29, Guidelines on the implementation of the Court of Justice of the European Union judgment on «Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González» [Linee guida relative all'esecuzione della sentenza della Corte di giustizia dell'Unione europea nella causa «Google Spain et Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González»], C-131/12, WP 225, 26 novembre 2014, pag. 23.

[10] CGUE, causa C-136/17, Commission nationale de l'informatique et des libertés (CNIL) contro Google LLC, sentenza del 24 settembre 2019.

[11] Direttiva 95/46/CE, articolo 14: «*Gli Stati membri riconoscono alla persona interessata il diritto: a) almeno nei casi di cui all'articolo 7, lettere e) e f), di opporsi in qualsiasi momento, per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano, salvo disposizione contraria prevista dalla normativa nazionale. In caso di opposizione giustificata il trattamento effettuato dal responsabile non può più riguardare tali dati*».

[12] In particolare, l'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (codificazione).

[13] CGUE, C-131/12, sentenza del 13 maggio 2014, punto 81; CGUE, C-136/17, sentenza del 24 settembre 2019, punto 66.

[14] CGUE, causa C-131/12, sentenza del 13 maggio 2014, punto 99; CGUE, causa C-136/17, sentenza del 24 settembre 2019, punto 53.

[15] CGUE, causa C-136/17, sentenza del 24 settembre 2019, punto 56 e seguenti

[16] CGUE, causa C-136/17, sentenza del 24 settembre 2019, punto 57.

[17] CGUE, causa C-136/17, sentenza del 24 settembre 2019, punto 59.

[18] CGUE, causa C-136/17, sentenza del 24 settembre 2019, punto 69.

[19] RGPD, articolo 6, paragrafo 3: «La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:
a) dal diritto dell'Unione; o
b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento (...)».

Torna a **Indice** | **Premessa**

Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679 - Versione 1.1

Adottate il 4 maggio 2020

Cronologia delle versioni

Versione 1.1	13 maggio 2020	Correzioni di formattazione
Versione 1.0	4 maggio 2020	Adozione delle linee guida

Indice

0. Prefazione

1. Introduzione

2. Consenso di cui all'articolo 4, punto 11, del regolamento generale sulla protezione dei dati

3. Elementi del consenso valido
   - 3.1 Consenso libero/manifestazione di volontà libera
     - 3.1.1 Squilibrio di potere
     - 3.1.2 Condizionalità
     - 3.1.3 Granularità
     - 3.1.4 Pregiudizio
   - 3.2 Specifico
   - 3.3 Informato
     - 3.3.1 Requisiti minimi di contenuto del consenso "informato"
     - 3.3.2 Come fornire le informazioni
   - 3.4 Manifestazione di volontà inequivocabile

4. Ottenimento del consenso esplicito

5. Condizioni aggiuntive per l'ottenimento di un consenso valido
   - 5.1 Dimostrazione del consenso
   - 5.2 Revoca del consenso

6. Interazione tra il consenso e altre basi legittime di cui all'articolo 6 del regolamento generale sulla protezione dati

7. Settori specifici di interesse nel regolamento generale sulla protezione dei dati
   - 7.1 Minori (articolo 8)
     - 7.1.1 Servizio della società dell'informazione
     - 7.1.2 Forniti direttamente a un minore
     - 7.1.3 Età
     - 7.1.4 Consenso del minore e responsabilità genitoriale
   - 7.2 Ricerca scientifica
   - 7.3 Diritti dell'interessato

8 Consenso ottenuto a norma della direttiva 95/46/CE

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati),

visto l'accordo sullo Spazio economico europeo (SEE), in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

viste le linee guida sul consenso ai sensi del regolamento (UE) 2016/679 adottate dal Gruppo di lavoro Articolo 29 (WP259 rev.01),

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

0. PREFAZIONE

Il 10 aprile 2018 il Gruppo di lavoro Articolo 29 ha adottato le linee guida sul consenso ai sensi del regolamento (UE) 2016/679 (WP259.01), che il Comitato europeo per la protezione dei dati ("Comitato") ha approvato nel corso della sua prima riunione plenaria. Il presente documento è una versione leggermente aggiornata di tali linee guida. Qualsiasi riferimento alle linee guida sul consenso elaborate dal Gruppo di lavoro Articolo 29 (WP259 rev.01) dovrebbe d'ora in poi essere inteso come riferimento alle presenti linee guida.

Il Comitato ha rilevato la necessità di ulteriori chiarimenti, in particolare per quanto riguarda due aspetti:

1 la validità del consenso espresso dall'interessato nell'interagire con i cosiddetti "cookie walls";

2 l'esempio 16 sullo scorrimento ("scrolling") e il consenso.

I punti relativi a questi due aspetti sono stati rivisti e aggiornati, mentre il resto del documento è rimasto invariato, fatta eccezione per alcune modifiche redazionali. La revisione riguarda più specificamente:

- la sezione relativa alla Condizionalità (punti 38 - 41);
- la sezione relativa alla Manifestazione di volontà inequivocabile (punto 86).

1. INTRODUZIONE

1. Le presenti linee guida forniscono un'analisi approfondita della nozione di consenso di cui al regolamento (UE) 2016/679 ("regolamento generale sulla protezione dei dati" o "regolamento"). Il concetto di consenso di cui alla direttiva sulla protezione dei dati (direttiva 95/46/CE) e alla direttiva relativa alla vita privata e alle comunicazioni elettroniche (direttiva 2002/58/CE) si è evoluto. Il regolamento generale sulla protezione dei dati fornisce ulteriori chiarimenti e specifiche sui requisiti per ottenere e dimostrare un consenso valido. Prendendo le mosse dal parere 15/2011 del Gruppo di lavoro Articolo 29 sul consenso, le presenti linee guida si concentrano sui cambiamenti introdotti, fornendo orientamenti pratici per garantire il rispetto del regolamento. Il titolare del trattamento è tenuto a innovare per trovare soluzioni che siano conformi ai requisiti di legge e sostengano meglio la protezione dei dati personali e gli interessi degli interessati.
2. Il consenso rimane una delle sei basi legittime per trattare i dati personali, come disposto dall'articolo 6 del regolamento[2]. Prima di avviare attività che implicano il trattamento di dati personali, il titolare del trattamento deve sempre valutare con attenzione la base legittima appropriata per il trattamento.
3. Di norma il consenso può costituire la base legittima appropriata solo se all'interessato vengono offerti il controllo e l'effettiva possibilità di scegliere se accettare i termini proposti o rifiutarli senza subire pregiudizio. Quando richiede il consenso, il titolare del trattamento deve valutare se questo sod-

disferà tutti i requisiti per essere valido. Se ottenuto nel pieno rispetto del regolamento, il consenso è uno strumento che fornisce all'interessato il controllo sul trattamento dei dati personali che lo riguardano. In caso contrario, il controllo diventa illusorio e il consenso non costituirà una base valida per il trattamento, rendendo illecita l'attività di trattamento[3].

4. Ove coerenti con il nuovo quadro giuridico, i pareri che il Gruppo di lavoro Articolo 29 ha formulato in materia di consenso[4] rimangono pertinenti, in quanto il regolamento generale sulla protezione dei dati codifica gli orientamenti e le buone prassi generali del Gruppo di lavoro Articolo 29 e lascia immutata la maggior parte degli aspetti essenziali del consenso. Di conseguenza, il presente documento del Comitato amplia e integra precedenti pareri del Gruppo di lavoro Articolo 29 su argomenti specifici che fanno riferimento al consenso ai sensi della direttiva 95/46/CE, senza sostituirli.

5. Come affermato dal Gruppo di lavoro Articolo 29 nel parere 15/2011 sulla definizione di consenso, l'invito ad accettare il trattamento dei dati dovrebbe essere soggetto a criteri rigorosi, poiché sono in gioco i diritti fondamentali dell'interessato e il titolare del trattamento intende svolgere un trattamento che senza il consenso sarebbe illecito[5]. Il ruolo cruciale del consenso è sottolineato dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Inoltre, l'ottenimento del consenso non fa venir meno né diminuisce in alcun modo l'obbligo del titolare del trattamento di rispettare i principi applicabili al trattamento sanciti nel regolamento generale sulla protezione dei dati, in particolare all'articolo 5, per quanto concerne la correttezza, la necessità e la proporzionalità, nonché la qualità dei dati. Il fatto che il trattamento dei dati personali si basi sul consenso dell'interessato non legittima la raccolta di dati non necessari a una finalità specifica di trattamento, che sarebbe fondamentalmente iniqua[6].

6. Parallelamente, il Comitato è a conoscenza della revisione della direttiva relativa alla vita privata e alle comunicazioni elettroniche. La nozione di consenso nel progetto di regolamento sulla vita privata e le comunicazioni elettroniche rimane legata a quella del regolamento generale sulla protezione dei dati[7]. È probabile che ai sensi del futuro strumento le organizzazioni necessitino del consenso per la maggior parte dei messaggi di marketing online, per le chiamate di marketing e per i metodi di tracciamento online, compreso tramite l'uso di cookie, applicazioni o altri software. Il Comitato ha già fornito raccomandazioni e orientamenti al legislatore europeo in merito alla proposta di regolamento sulla vita privata e le comunicazioni elettroniche[8].

7. Per quanto riguarda l'attuale direttiva relativa alla vita privata e alle comunicazioni elettroniche, il Comitato rileva che i riferimenti alla direttiva 95/46/CE abrogata si intendono fatti al regolamento generale sulla protezione dei dati[9]. Ciò vale anche per i riferimenti riguardanti il consenso, poiché il regolamento sulla vita privata e le comunicazioni elettroniche non sarà (ancora) entrato in vigore il 25 maggio 2018. Ai sensi dell'articolo 95 del regolamento generale sulla protezione dei dati, non sono imposti obblighi supplementari in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione,

nella misura in cui la direttiva relativa alla vita privata e alle comunicazioni elettroniche impone obblighi specifici aventi il medesimo obiettivo. Il Comitato rileva che i requisiti per il consenso ai sensi del regolamento generale sulla protezione dei dati non sono considerati un "obbligo supplementare", bensì condizioni preliminari per la liceità del trattamento. Pertanto, tali requisiti sono applicabili alle situazioni che rientrano nel campo di applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

2. CONSENSO DI CUI ALL'ARTICOLO 4, PUNTO 11, DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

8. L'articolo 4, punto 11, del regolamento generale sulla protezione dei dati definisce il consenso dell'interessato come: "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*".

9. La nozione di consenso rimane sostanzialmente simile a quella della direttiva 95/46/CE, e il consenso rimane uno dei presupposti per il trattamento dei dati personali, ai sensi dell'articolo 6 del regolamento generale sulla protezione dei dati[10]. Oltre alla definizione modificata di cui all'articolo 4, punto 11, il regolamento fornisce ulteriori indicazioni, all'articolo 7 e ai considerando 32, 33, 42 e 43, su come il titolare del trattamento deve agire per rispettare gli elementi principali del requisito del consenso.

10. L'inclusione, nel regolamento, di disposizioni e considerando specifici sulla revoca del consenso conferma che quest'ultimo dovrebbe essere una decisione reversibile e che l'interessato mantiene un certo grado di controllo.

3. ELEMENTI DEL CONSENSO VALIDO

11. L'articolo 4, punto 11, del regolamento generale sulla protezione dei dati stabilisce che il consenso dell'interessato è qualsiasi:

- manifestazione di volontà libera,
- specifica,
- informata e
- inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

12. Le sezioni che seguono analizzano la misura in cui la formulazione dell'articolo 4, punto 11, richiede al titolare del trattamento di modificare le sue richieste/i suoi moduli di consenso affinché siano conformi al regolamento generale sulla protezione dei dati[11].

3.1 CONSENSO LIBERO/MANIFESTAZIONE DI VOLONTÀ LIBERA[12]

13. L'elemento della manifestazione di volontà "libera" implica che l'interessato abbia una scelta effettiva e il controllo sui propri dati. Come regola generale, il regolamento stabilisce che se l'interessato non dispone di una scelta effettiva o si sente obbligato ad acconsentire oppure subirà conseguenze negative se non acconsente, il consenso non sarà valido[13]. Se il consenso è un elemento non negoziabile delle condizioni generali di contratto/servizio, si presume che non sia stato prestato liberamente. Di conseguenza, il consenso non sarà considerato libero se l'interessato non può rifiutarlo o revocarlo senza subire pregiudizio[14]. Il regolamento generale sulla protezione dei dati ha preso in considerazione anche la nozione di squilibrio tra titolare del trattamento e interessato.
14. Nel valutare se il consenso sia stato prestato liberamente, si deve anche tener conto dell'eventualità che il consenso sia collegato all'esecuzione di un contratto o alla prestazione di un servizio come descritto all'articolo 7, paragrafo 4. L'articolo 7, paragrafo 4, contenendo l'inciso "tra le altre", non è esaustivo e può quindi comprendere altre eventualità. In termini generali, qualsiasi azione di pressione o influenza inappropriata sull'interessato (che si può manifestare in vari modi) che impedisca a quest'ultimo di esercitare il suo libero arbitrio, rende il consenso invalido.

15. Esempio 1: Un'applicazione mobile per il fotoritocco chiede agli utenti di attivare la localizzazione GPS per l'utilizzo dei suoi servizi. L'applicazione comunica agli utenti che utilizzerà i dati raccolti per finalità di pubblicità comportamentale. Né la geolocalizzazione né la pubblicità comportamentale online sono necessarie per la prestazione del servizio di fotoritocco e vanno oltre la fornitura del servizio principale. Poiché gli utenti non possono utilizzare l'applicazione senza acconsentire a tali finalità, il consenso non può essere considerato liberamente espresso.

3.1.1. SQUILIBRIO DI POTERE

16. Il considerando 43[15] indica chiaramente che è improbabile che le autorità pubbliche possano basarsi sul consenso per effettuare il trattamento, poiché quando il titolare del trattamento è un'autorità pubblica sussiste spesso un evidente squilibrio di potere nella relazione tra il titolare del trattamento e l'interessato. In molti di questi casi è inoltre evidente che l'interessato non dispone di alternative realistiche all'accettazione (dei termini) del trattamento. Il Comitato ritiene che esistano altre basi legittime, in linea di principio più appropriate, per il trattamento da parte delle autorità pubbliche[16].
17. Fatte salve queste considerazioni generali, il regolamento non esclude completamente il ricorso al consenso come base legittima per il trattamento dei dati da parte delle autorità pubbliche. I seguenti esempi mostrano infatti che l'uso del consenso può essere appropriato in determinate circostanze.

18. Esempio 2: Un comune sta pianificando l'esecuzione di lavori di manutenzione stradale. Poiché i lavori possono perturbare il traffico per parecchio tempo, il comune offre ai cittadini la possibilità di iscriversi a una mailing list per ricevere aggiornamenti sull'avanzamento dei lavori e sui ritardi previsti. Il comune chiarisce che la partecipazione non è obbligatoria e chiede il consenso a utilizzare gli indirizzi di posta elettronica per questa finalità (esclusiva). I cittadini che non acconsentono non perderanno l'accesso ad alcun servizio fondamentale del comune né alcun diritto, di conseguenza possono esprimere o rifiutare liberamente il loro consenso a questo uso dei dati. Tutte le informazioni sui lavori stradali saranno disponibili anche sul sito web del comune.

19. Esempio 3: Un proprietario terriero necessita di alcuni permessi tanto dal comune quanto dalla provincia. Entrambi gli enti pubblici richiedono le stesse informazioni per il rilascio dei permessi, ma non hanno accesso alle rispettive banche dati. Di conseguenza entrambi chiedono le stesse informazioni e il proprietario terriero invia i dati ad entrambi. Il comune e la provincia chiedono il consenso dell'interessato per riunire i fascicoli al fine di evitare duplicazioni di procedure e corrispondenza. Entrambi gli enti pubblici assicurano che ciò è facoltativo e che le richieste di permesso verranno comunque trattate separatamente qualora l'interessato decida di non acconsentire alla riunione dei fascicoli. Il proprietario terriero può quindi esprimere liberamente il consenso alle autorità per la finalità di riunione dei fascicoli.

20. Esempio 4: Una scuola pubblica chiede agli studenti il consenso ad utilizzare le loro fotografie in una rivista studentesca in formato cartaceo. In questo caso il consenso costituisce una scelta vera e propria a condizione che agli studenti non vengano negati l'istruzione o altri servizi e che gli studenti possano rifiutare il consenso senza subire pregiudizio[17].

21. Lo squilibrio di potere sussiste anche nel contesto dell'**occupazione**[18]. Data la dipendenza risultante dal rapporto datore di lavoro/dipendente, è improbabile che l'interessato sia in grado di negare al datore di lavoro il consenso al trattamento dei dati senza temere o rischiare di subire ripercussioni negative come conseguenza del rifiuto. È improbabile che il dipendente sia in grado di rispondere liberamente, senza percepire pressioni, alla richiesta del datore di lavoro di acconsentire, ad esempio, all'attivazione di sistemi di monitoraggio, quali la sorveglianza con telecamere sul posto di lavoro, o alla compilazione di moduli di valutazione[19]. Di conseguenza il Comitato ritiene problematico per il datore di lavoro trattare i dati personali dei dipendenti attuali o futuri sulla base del consenso, in quanto è improbabile che questo venga prestato liberamente. Per la maggior parte delle attività di trattamento svolte sul posto di lavoro, la base legittima non può e non dovrebbe essere il

consenso del dipendente (articolo 6, paragrafo 1, lettera a)) in considerazione della natura del rapporto tra datore di lavoro e dipendente[20].

22. Tuttavia, ciò non significa che il datore di lavoro non possa mai basarsi sul consenso come base legittima per il trattamento. In alcune situazioni il datore di lavoro è in grado di dimostrare che il consenso è stato effettivamente espresso liberamente. Dato lo squilibrio di potere tra il datore di lavoro e il suo personale, i dipendenti possono manifestare il loro consenso liberamente soltanto in casi eccezionali, quando non subiranno alcuna ripercussione negativa per il fatto che esprimano il loro consenso o meno[21].

23. Esempio 5: Una troupe cinematografica filmerà una determinata area di un ufficio. Il datore di lavoro chiede a tutti i dipendenti che hanno la scrivania in quella zona il consenso a essere ripresi, in quanto potrebbero apparire sullo sfondo del video. Chi non vuole essere filmato non viene penalizzato in alcun modo e ottiene invece una scrivania altrove nell'edificio per l'intera durata delle riprese.

24. Gli squilibri di potere non sono limitati alle autorità pubbliche e ai datori di lavoro, potendo verificarsi anche in altre situazioni. Come evidenziato dal Comitato in diversi pareri, il consenso è valido soltanto se l'interessato è in grado di operare realmente una scelta e non c'è il rischio di raggiri, intimidazioni, coercizioni o conseguenze negative significative (ad es. costi aggiuntivi sostanziali) in caso di rifiuto a prestare il consenso. Il consenso non sarà considerato liberamente espresso qualora vi sia qualsiasi elemento di costrizione, pressione o incapacità di esercitare il libero arbitrio.

3.1.2 CONDIZIONALITÀ

25. Per valutare se il consenso sia stato prestato liberamente è di rilievo l'articolo 7, paragrafo 4, del regolamento[22].

26. L'articolo 7, paragrafo 4, indica, tra l'altro, che è altamente inopportuno "accorpare" il consenso all'accettazione delle condizioni generali di contratto/servizio o "subordinare" la fornitura di un contratto o servizio a una richiesta di consenso al trattamento di dati personali che non sono necessari per l'esecuzione del contratto o servizio. Si presume che il consenso prestato in una tale situazione non sia stato espresso liberamente (considerando 43). L'articolo 7, paragrafo 4, mira a garantire che la finalità del trattamento dei dati personali non sia mascherata né accorpata all'esecuzione di un contratto o alla prestazione di un servizio per il quale i dati personali non sono necessari. In tal modo, il regolamento assicura che il trattamento dei dati personali per cui viene richiesto il consenso non possa trasformarsi direttamente o indirettamente in una controprestazione contrattuale. Le due basi legittime per la liceità del trattamento dei dati personali, ossia il consenso e l'esecuzione di un contratto, non possono essere riunite e rese indistinte.

27. L'obbligo di acconsentire all'uso di dati personali aggiuntivi rispetto a quelli strettamente necessari limita la scelta dell'interessato e ostacola l'espressione del libero consenso. Poiché la legislazione in materia di protezione dei dati mira a tutelare i diritti fondamentali, è essenziale che l'interessato abbia il controllo sui propri dati personali; inoltre sussiste una presunzione forte secondo cui il consenso a un trattamento di dati personali non necessario non può essere considerato un corrispettivo obbligatorio dell'esecuzione di un contratto o della prestazione di un servizio.

28. Pertanto, ogni volta che una richiesta di consenso è legata all'esecuzione di un contratto da parte del titolare del trattamento, l'interessato che non desidera mettere a disposizione i propri dati personali per il trattamento da parte del titolare corre il rischio di vedersi negare l'erogazione dei servizi richiesti.

29. Per valutare se si verifica una situazione di accorpamento o subordinazione è importante determinare qual è la portata del contratto e quali dati sono necessari per la sua esecuzione.

30. Secondo il parere 6/2014 del Gruppo di lavoro Articolo 29, l'espressione "necessario per l'esecuzione di un contratto" deve essere interpretata in maniera rigorosa. Il trattamento deve essere necessario per adempiere il contratto con ciascun interessato. In quest'ambito possono rientrare, per esempio, il trattamento dell'indirizzo dell'interessato ai fini della consegna delle merci acquistate online o il trattamento degli estremi della carta di credito per facilitare il pagamento. Nel contesto occupazionale, questo presupposto potrebbe permettere, per esempio, il trattamento di informazioni riguardanti lo stipendio e le coordinate bancarie per consentire il pagamento degli stipendi[23]. È necessario che vi sia un collegamento diretto e obiettivo tra il trattamento dei dati e la finalità dell'esecuzione del contratto.

31. Quando il titolare del trattamento intende trattare dati personali che sono effettivamente necessari per l'esecuzione di un contratto il consenso non è la base legittima appropriata[24].

32. L'articolo 7, paragrafo 4, è pertinente soltanto laddove i dati richiesti **non** sono necessari per l'esecuzione del contratto (ivi compreso per la prestazione di un servizio) e l'esecuzione del contratto è subordinata all'ottenimento di tali dati in base al presupposto del consenso. Al contrario, qualora il trattamento **sia** necessario per eseguire il contratto (ivi incluso per la prestazione di un servizio), l'articolo 7, paragrafo 4, non si applica.

33. Esempio 6: Una banca chiede ai clienti il consenso per consentire a terzi di utilizzare i dettagli di pagamento per finalità di marketing diretto. Questa attività di trattamento non è necessaria per l'esecuzione del contratto stipulato con il cliente e la prestazione di servizi ordinari di conto bancario. Qualora il rifiuto del cliente a prestare il consenso per tale finalità di trattamento porti alla negazione di servizi bancari, alla chiusura del conto bancario o, a seconda dei casi, a un aumento della commissione, il consenso non può considerarsi espresso liberamente.

34. La scelta del legislatore di evidenziare la condizionalità, tra l'altro, come presunzione di mancanza di libertà di esprimere il consenso dimostra che il verificarsi della condizionalità deve essere attentamente esaminato. L'espressione "nella massima considerazione" di cui all'articolo 7, paragrafo 4, suggerisce che il titolare del trattamento deve prestare particolare attenzione qualora il contratto (che potrebbe includere la prestazione di un servizio) sia collegato a una richiesta di consenso al trattamento di dati personali.

35. Poiché l'articolo 7, paragrafo 4, non è formulato in maniera assoluta, in un numero molto ristretto di casi tale condizionalità potrebbe non rendere invalido il consenso. Tuttavia, il verbo "si presume" al considerando 43 indica chiaramente che tali casi saranno estremamente eccezionali.

36. Ad ogni modo, l'onere della prova riguardo all'articolo 7, paragrafo 4, incombe al titolare del trattamento[25]. Questa norma specifica riflette il principio generale di responsabilizzazione che permea l'intero regolamento generale sulla protezione dei dati. Tuttavia, quando si applica l'articolo 7, paragrafo 4, risulta più difficile per il titolare del trattamento dimostrare che l'interessato ha prestato liberamente il consenso[26].

37. Il titolare del trattamento potrebbe sostenere che la sua organizzazione offre all'interessato una scelta reale mettendolo in grado di scegliere tra un servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente che non implica un siffatto consenso, dall'altro. Finché esiste la possibilità che il contratto venga eseguito o che il servizio oggetto del contratto venga prestato dal titolare del trattamento senza necessità di acconsentire ad usi ulteriori o supplementari dei dati in questione non si è in presenza di un servizio condizionato. Tuttavia, i due servizi devono essere effettivamente equivalenti.

38. Il Comitato ritiene che il consenso non possa considerarsi prestato liberamente se il titolare del trattamento sostiene che esiste la possibilità di scegliere tra il suo servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente offerto da un altro titolare del trattamento, dall'altro. In tal caso la libertà di scelta dipenderebbe dagli altri operatori del mercato e dal fatto che l'interessato ritenga che i servizi offerti dall'altro titolare del trattamento siano effettivamente equivalenti. Ciò implicherebbe inoltre l'obbligo per i titolari del trattamento di monitorare gli sviluppi del mercato per garantire la continuità della validità del consenso per le rispettive attività di trattamento dei dati, in quanto un concorrente potrebbe successivamente modificare il servizio prestato. Pertanto, il ricorso a tale argomentazione significa che un consenso fondato sull'esistenza di un'opzione alternativa offerta da un terzo non è conforme al regolamento generale sulla protezione dei dati, e pertanto un prestatore di servizi non può impedire all'interessato di accedere a un servizio per il fatto che questi non ha prestato il proprio consenso.

39. Affinché il consenso sia prestato liberamente, l'accesso ai servizi e alle funzionalità non deve essere subordinato al consenso dell'utente alla memorizzazione di informazioni o all'ottenimento dell'accesso a informazioni già memorizzate nell'apparecchiatura terminale dell'utente (i cosiddetti "cookie wall")[27].

40. Esempio 6 bis: Un fornitore di un sito web predispone uno script che blocca la visualizzazione del contenuto e fa apparire solo la richiesta di accettare i cookie, le informazioni sui cookie che verranno installati e le finalità per le quali i dati saranno trattati. Non è possibile accedere al contenuto senza cliccare sul pulsante "Accetto i cookie". Poiché all'interessato non è offerta una scelta effettiva, il suo consenso non è espresso liberamente.
41. In questo caso il consenso non è valido, in quanto la prestazione del servizio è subordinata al fatto che l'interessato clicchi sul pulsante "Accetto i cookie". Non è offerta una scelta effettiva.

3.1.3 GRANULARITÀ

42. Un servizio può comportare trattamenti multipli per più finalità. In tal caso, l'interessato dovrebbe essere libero di scegliere quale finalità accettare anziché dover acconsentire a un insieme di finalità. Ai sensi del regolamento generale sulla protezione dei dati, in un determinato caso possono essere giustificati più consensi per iniziare a offrire un servizio.
43. Il considerando 43 chiarisce che si presume che il consenso non sia stato espresso liberamente se il processo o la procedura seguiti per ottenerlo non permettono all'interessato di esprimere un consenso separato ai distinti trattamenti dei dati personali (ad esempio solo ad alcuni trattamenti e non ad altri) nonostante ciò sia appropriato nel singolo caso. Il considerando 32 afferma: *"Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste"*.
44. Se il titolare del trattamento ha riunito diverse finalità di trattamento e non ha chiesto il consenso separato per ciascuna di esse non c'è libertà. La granularità è strettamente correlata alla necessità che il consenso sia specifico, come analizzato nella sezione 3.2. Quando il trattamento di dati mira a perseguire finalità diverse, la soluzione per soddisfare le condizioni per la validità del consenso risiede nella granularità, ossia nella separazione delle finalità e nell'ottenimento del consenso per ciascuna di esse.

45. Esempio 7: Nel contesto della medesima richiesta di consenso, un rivenditore chiede ai propri clienti il consenso a utilizzare i loro dati per inviare comunicazioni di marketing tramite posta elettronica e per condividere i dati con altre società del gruppo. Tale consenso non è granulare in quanto non è distinto per queste due finalità, pertanto non sarà valido. In questo caso è necessario un consenso specifico all'invio dei dati di contatto ai partner commerciali. Tale consenso specifico sarà ritenuto valido per ciascun partner (cfr. anche la sezione 3.3.1) la cui identità è stata fornita all'interessato al momento

dell'ottenimento del consenso, nella misura in cui i dati vengano inviati per la medesima finalità (nell'esempio, finalità di marketing).

3.1.4 PREGIUDIZIO

46. Il titolare del trattamento deve dimostrare che è possibile rifiutare il consenso oppure revocarlo senza subire pregiudizio (considerando 42), ad esempio dimostrando che la revoca del consenso non comporta alcun costo per l'interessato e quindi nessuno svantaggio evidente in caso di revoca.
47. Altri esempi di pregiudizio sono l'inganno, l'intimidazione, la coercizione o conseguenze negative significative in caso di mancato consenso. Il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha potuto scegliere liberamente o realmente se acconsentire o meno e che poteva revocare il consenso senza pregiudizio.
48. Se il titolare del trattamento può dimostrare che il servizio consente di revocare il consenso senza conseguenze negative, ad esempio senza che il livello della prestazione del servizio venga diminuito a scapito dell'utente, allora può dimostrare che il consenso è stato conferito liberamente. Il regolamento generale sulla protezione dei dati non esclude tutti gli incentivi, tuttavia spetta al titolare del trattamento dimostrare che il consenso è stato prestato liberamente in tutte le circostanze.

49. Esempio 8: Un'applicazione mobile dedicata allo stile di vita richiede, all'atto dello scaricamento, il consenso all'accesso all'accelerometro del telefono. Tale accesso non è necessario per il funzionamento dell'applicazione, ma è utile al titolare del trattamento per saperne di più sui movimenti e sui livelli di attività degli utenti. Un utente revoca il consenso e scopre che dopo la revoca l'applicazione funziona solo in misura limitata. Questo è un esempio di pregiudizio ai sensi del considerando 42, il che significa che il consenso non è mai stato ottenuto in maniera valida (e quindi il titolare del trattamento deve cancellare tutti i dati personali sui movimenti degli utenti raccolti in tale modo).

50. Esempio 9: Un interessato si iscrive alla newsletter di un rivenditore del settore della moda che offre sconti generali. Il rivenditore chiede all'interessato il consenso per raccogliere ulteriori dati sulle preferenze di acquisto in maniera da personalizzare le offerte in base alle preferenze dell'interessato secondo la cronologia degli acquisti o un questionario facoltativo. Quando l'interessato successivamente revoca il consenso, riceve nuovamente sconti per articoli di moda non personalizzati. Ciò non equivale a un pregiudizio in quanto l'interessato ha perso soltanto l'incentivo ammissibile.

51. Esempio 10: Una rivista di moda offre ai lettori la possibilità di acquistare nuovi prodotti per il trucco prima del loro lancio ufficiale.
52. I prodotti saranno presto disponibili per la vendita, ma i lettori della rivista ne riceveranno un'anteprima esclusiva. Per godere di tale vantaggio i lettori devono fornire l'indirizzo postale e accettare l'iscrizione alla mailing list della rivista. L'indirizzo postale è necessario per la spedizione e la mailing list viene utilizzata per l'invio di offerte commerciali per prodotti quali cosmetici o t-shirt nel corso dell'anno.
53. L'azienda spiega che i dati relativi alla mailing list saranno utilizzati esclusivamente per l'invio di prodotti e pubblicità cartacea da parte della rivista stessa e non saranno condivisi con altre organizzazioni.
54. Qualora non voglia comunicare il proprio indirizzo per tale finalità, il lettore non subisce alcun pregiudizio in quanto i prodotti saranno comunque a sua disposizione.

3.2 SPECIFICO

55. L'articolo 6, paragrafo 1, lettera a), conferma che il consenso dell'interessato deve essere espresso in relazione a "una o più specifiche" finalità e che l'interessato deve poter scegliere in relazione a ciascuna di esse[28]. Il requisito secondo il quale il consenso deve essere "specifico" mira a garantire un certo grado di controllo da parte dell'utente e trasparenza per l'interessato. Tale requisito non è stato modificato dal regolamento e rimane strettamente legato al requisito del consenso "informato". Allo stesso tempo, deve essere interpretato in linea con il requisito della "granularità", affinché il consenso sia "libero"[29]. In sintesi, per rispettare l'elemento della specificità ("specifico"), il titolare del trattamento deve applicare:
    i. la specificazione delle finalità come garanzia contro la "function creep", ossia l'estensione indebita delle funzionalità;
    ii. la granularità nelle richieste di consenso, e
    iii. una chiara separazione delle informazioni sull'ottenimento del consenso per le attività di trattamento dei dati rispetto alle informazioni su altre questioni.
56. **Sul punto i)**: ai sensi dell'articolo 5, paragrafo 1, lettera b), del regolamento, per ottenere un consenso valido occorre sempre prima determinare la finalità specifica, esplicita e legittima dell'attività di trattamento prevista[30]. La necessità di un consenso specifico associata alla nozione di limitazione delle finalità di cui all'articolo 5, paragrafo 1, lettera b), funge da garanzia contro l'ampliamento progressivo, o la commistione, delle finalità di trattamento dei dati dopo che l'interessato ha acconsentito alla loro raccolta iniziale. Questo fenomeno, noto anche come "function creep", rappresenta un rischio per l'interessato, in quanto può comportare l'uso non previsto di dati perso-

nali da parte del titolare del trattamento o di terzi e la perdita del controllo da parte dell'interessato.

57. Se il titolare del trattamento si basa sull'articolo 6, paragrafo 1, lettera a), l'interessato deve sempre fornire il consenso per una finalità di trattamento specifica[31]. In linea con il concetto di *limitazione delle finalità* e con l'articolo 5, paragrafo 1, lettera b), e il considerando 32 del regolamento, il consenso può coprire trattamenti distinti, purché abbiano la medesima finalità. Chiaramente il consenso specifico può essere ottenuto soltanto quando l'interessato è specificamente informato delle finalità previste dell'uso dei dati che lo riguardano.

58. Nonostante le disposizioni in materia di compatibilità delle finalità, il consenso deve essere specifico per finalità. L'interessato presterà il consenso nella convinzione di avere il controllo sui suoi dati e nella convinzione che questi saranno trattati esclusivamente per le finalità specificate. Se tratta i dati basandosi sul presupposto del consenso e intende trattarli per un'altra finalità, il titolare del trattamento deve richiedere un ulteriore consenso per tale finalità a meno che non possa basarsi su un'altra base legittima che risponda meglio alla situazione.

59. Esempio 11: Una rete TV via cavo raccoglie i dati personali degli abbonati, sulla base del loro consenso, per fornire suggerimenti personali su nuovi film che, stando alle abitudini di visualizzazione, potrebbero interessare loro. Dopo un po', la rete TV vorrebbe consentire a terzi di inviare (o mostrare) pubblicità mirata sulla base delle abitudini di visualizzazione degli abbonati. Data questa nuova finalità, è necessario ottenere un nuovo consenso.

60. **Sul punto ii)**: i meccanismi di consenso devono essere granulari non solo per soddisfare il requisito del consenso "libero", ma anche per soddisfare quello del consenso "specifico". Ciò significa che il titolare del trattamento che richiede il consenso per finalità diverse dovrebbe prevedere una possibilità di adesione distinta per ciascuna finalità, in modo da consentire all'utente di esprimere un consenso specifico per le finalità specifiche.

61. **Sul punto iii)**: il titolare del trattamento dovrebbe fornire informazioni specifiche, in relazione a ciascuna richiesta di consenso distinta, sui dati che vengono trattati per ciascuna finalità, al fine di rendere noto all'interessato l'impatto delle diverse scelte a sua disposizione. In questo modo l'interessato può esprimere un consenso specifico. Questo aspetto si sovrappone al requisito che impone al titolare del trattamento di fornire informazioni chiare, come analizzato al punto 3.3.

3.3 INFORMATO

62. Il regolamento generale sulla protezione dei dati rafforza il requisito secondo cui il consenso deve essere informato. Ai sensi dell'articolo 5 del regolamento, il requisito della trasparenza è uno dei principi fondamentali, strettamente legato ai principi di correttezza e liceità. Fornire informazioni agli interessati prima di ottenerne il consenso è fondamentale per consentire loro di prendere decisioni informate, capire a cosa stanno acconsentendo e, ad esempio, esercitare il diritto di revocare il consenso. Se il titolare del trattamento non fornisce informazioni accessibili, il controllo dell'utente diventa illusorio e il consenso non costituirà una base valida per il trattamento.
63. Se i requisiti per il consenso informato non sono rispettati il consenso non sarà valido e il titolare del trattamento potrebbe essere in violazione dell'articolo 6 del regolamento.

3.3.1 REQUISITI MINIMI DI CONTENUTO DEL CONSENSO "INFORMATO"

64. Affinché il consenso sia informato è necessario informare l'interessato su determinati elementi che sono fondamentali per effettuare una scelta. Di conseguenza, il Comitato ritiene che per ottenere un consenso valido siano necessarie almeno le seguenti informazioni:
    i. l'identità del titolare del trattamento[32];
    ii. la finalità di ciascuno dei trattamenti per i quali è richiesto il consenso[33];
    iii. quali (tipi di) dati saranno raccolti e utilizzati[34];
    iv. l'esistenza del diritto di revocare il consenso[35];
    v. informazioni sull'uso dei dati per un processo decisionale automatizzato ai sensi dell'articolo 22, paragrafo 2, lettera c)[36], se del caso; e
    vi. informazioni sui possibili rischi di trasferimenti di dati dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate come descritto nell'articolo 46[37].
65. Per quanto riguarda i punti i) e iii), il Comitato osserva che qualora più titolari del trattamento (congiunti) intendano basarsi sul medesimo consenso oppure qualora i dati debbano essere trasferiti o trattati da altri titolari del trattamento che intendono basarsi sul consenso iniziale, tutti questi titolari del trattamento devono essere indicati. Non è necessario fornire i nomi dei responsabili del trattamento, sebbene per rispettare gli articoli 13 e 14 del regolamento il titolare del trattamento dovrà fornire un elenco completo dei destinatari o delle categorie di destinatari, inclusi i responsabili del trattamento. Per concludere, il Comitato rileva che, a seconda delle circostanze e del contesto della fattispecie, potrebbero essere necessarie più informazioni per consentire all'interessato di comprendere veramente i trattamenti in corso.

3.3.2 COME FORNIRE LE INFORMAZIONI

66. Il regolamento generale sulla protezione dei dati non prescrive la forma o il formato in cui è necessario fornire le informazioni affinché sia soddisfatto il requisito del consenso informato. Le informazioni valide possono quindi essere presentate in vari modi, ad esempio sotto forma di dichiarazioni scritte o verbali oppure di messaggi audio o video. Tuttavia, il regolamento prevede varie prescrizioni in merito al consenso informato, in particolare all'articolo 7, paragrafo 2, e al considerando 32. Ciò assicura un maggiore livello di chiarezza e accessibilità delle informazioni.

67. Quando richiede il consenso, il titolare del trattamento dovrebbe assicurarsi di usare sempre un linguaggio chiaro e semplice. Ciò significa che il messaggio dovrebbe essere facilmente comprensibile per una persona media, non solo per un avvocato. Il titolare del trattamento non può usare lunghe politiche sulla tutela della vita privata difficili da comprendere oppure informative piene di gergo giuridico. Il consenso deve essere chiaro e distinguibile dalle altre questioni, e deve essere presentato in una forma intelligibile e facilmente accessibile. Ciò significa, in sostanza, che le informazioni pertinenti per prendere una decisione informata sul consenso non possono essere nascoste all'interno delle condizioni generali di contratto/servizio[38].

68. Il titolare del trattamento deve garantire che il consenso sia fornito sulla base di informazioni che consentono all'interessato di identificare facilmente chi è il titolare del trattamento e di capire a cosa sta acconsentendo. Il titolare del trattamento deve descrivere chiaramente la finalità del trattamento dei dati per la quale richiede il consenso[39].

69. Ulteriori orientamenti specifici in materia di accessibilità sono stati forniti dal Gruppo di lavoro Articolo 29 nelle linee guida sulla trasparenza. Quando il consenso deve essere prestato per via elettronica, la richiesta deve essere chiara e concisa. La messa a disposizione di informazioni "a livelli" e granulari può essere un modo appropriato per soddisfare il duplice obbligo di essere precisi e completi, da un lato, e comprensibili, dall'altro.

70. Il titolare del trattamento deve valutare il tipo di pubblico che fornisce dati personali alla sua organizzazione. Ad esempio, se il pubblico di destinazione include interessati minorenni, il titolare del trattamento deve assicurarsi che le informazioni siano comprensibili per i minori[40]. Dopo aver individuato il pubblico, il titolare del trattamento deve stabilire le informazioni da fornire e, successivamente, il modo in cui fornirle.

71. L'articolo 7, paragrafo 2, concerne le dichiarazioni scritte di consenso preformulate che riguardano anche altre questioni. Quando il consenso viene richiesto nell'ambito di un contratto (cartaceo), la richiesta di consenso deve essere chiaramente distinguibile dal resto. Se il contratto cartaceo tratta numerosi aspetti che non sono collegati al consenso all'uso dei dati personali, quest'ultimo deve essere trattato in modo da distinguersi chiaramente oppure in un documento distinto. Analogamente, ai sensi del considerando 32, se il consenso viene richiesto per via elettronica, la richiesta di consenso deve

essere separata e distinta, e non può semplicemente figurare in un paragrafo all'interno delle condizioni generali di contratto/servizio[41]. Per tener conto degli schermi di piccole dimensioni o degli spazi ristretti per le informazioni, può essere appropriata, se del caso, una modalità di visualizzazione delle informazioni "a livelli" per evitare eccessivi disturbi all'esperienza dell'utente o alla progettazione del prodotto.

72. Per rispettare il regolamento il titolare del trattamento che si basa sul consenso dell'interessato deve adempiere anche gli obblighi di informazione separati di cui agli articoli 13 e 14. Nella pratica il rispetto degli obblighi di informazione e del requisito del consenso informato possono portare in molti casi a un approccio integrato. Tuttavia la presente sezione è scritta nella consapevolezza che possa sussistere un consenso "informato" valido anche quando non tutti gli aspetti di cui agli articoli 13 e/o 14 sono menzionati nel processo di ottenimento del consenso (questi punti dovrebbero ovviamente essere menzionati altrove, come ad esempio nell'informativa sulla protezione dei dati personali dell'azienda). Il Gruppo di lavoro Articolo 29 ha emanato linee guida separate sul requisito della trasparenza.

73. Esempio 12: L'azienda X è un titolare del trattamento che ha ricevuto reclami per il fatto che agli interessati non è chiaro l'uso dei dati per il quale si chiede loro il consenso. L'azienda ritiene quindi sia necessario verificare se le informazioni contenute nella sua richiesta di consenso sono comprensibili per gli interessati. X organizza gruppi di prova volontari di categorie specifiche dei propri clienti e presenta loro nuovi aggiornamenti delle informazioni di consenso prima di comunicarle esternamente. La selezione di tale gruppo rispetta il principio di indipendenza ed avviene sulla base di norme che garantiscono un risultato rappresentativo e non distorto. Il gruppo riceve un questionario e indica cosa ha capito delle informazioni e quale valutazione darebbe sulla comprensibilità e pertinenza delle informazioni. Il titolare del trattamento continua a eseguire prove fino a quando i gruppi di prova non indicano che le informazioni sono comprensibili. X redige una relazione della prova e la tiene disponibile per riferimento futuro. Questo esempio mostra un modo con cui X può dimostrare che gli interessati hanno ricevuto informazioni chiare prima di acconsentire al trattamento dei loro dati personali da parte di X.

74. Esempio 13: Un'azienda effettua un trattamento di dati basandosi sul presupposto del consenso. L'azienda utilizza un'informativa sulla protezione dei dati a più livelli che include una richiesta di consenso. L'azienda comunica tutti i dettagli di base del titolare del trattamento e le attività di trattamento dei dati previste[42]. Tuttavia, l'azienda non indica in che modo sia possibile contattare il responsabile della protezione dei dati nel primo livello di informazioni dell'informativa. Ai fini della base legittima e valida per il trattamento ai sensi dell'articolo 6, questo titolare del trattamento ha ottenuto un consenso "infor-

mato" valido, anche se i dati di contatto del responsabile della protezione dei dati non sono stati comunicati all'interessato (nel primo livello di informazioni), a norma dell'articolo 13, paragrafo 1, lettera b) o dell'articolo 14, paragrafo 1, lettera b).

3.4 MANIFESTAZIONE DI VOLONTÀ INEQUIVOCABILE

75. Il regolamento generale sulla protezione dei dati afferma chiaramente che il consenso richiede una dichiarazione o un'azione positiva inequivocabile da parte dell'interessato, il che significa che il consenso deve sempre essere espresso attraverso una dichiarazione o in modo attivo. Deve essere ovvio che l'interessato ha acconsentito al particolare trattamento.

76. L'articolo 2, lettera h), della direttiva 95/46/CE definisce il consenso come una "manifestazione di volontà con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento". L'articolo 4, punto 11, del regolamento generale sulla protezione dei dati si basa su tale definizione, chiarendo che il consenso, per essere valido, richiede una manifestazione *inequivocabile* mediante una *dichiarazione o azione positiva inequivocabile*, in conformità alle precedenti linee guida del Gruppo di lavoro Articolo 29.

77. Con "azione positiva inequivocabile" si intende che l'interessato deve aver intrapreso un'azione deliberata per acconsentire al trattamento specifico[43]. Il considerando 32 stabilisce ulteriori orientamenti al riguardo. Il consenso può essere raccolto attraverso una dichiarazione scritta o verbale (registrata), anche tramite mezzi elettronici.

78. Probabilmente il modo più rigoroso per soddisfare il criterio della "dichiarazione scritta" consiste nell'assicurarsi che l'interessato scriva una lettera o un messaggio di posta elettronica al titolare del trattamento spiegando ciò a cui acconsente esattamente. Tuttavia, spesso ciò non è realistico. Le dichiarazioni scritte possono avere forme e formati diversi che potrebbero essere conformi al regolamento generale sulla protezione dei dati.

79. Fatto salvo il diritto contrattuale (nazionale) in vigore, il consenso può essere ottenuto attraverso una dichiarazione verbale registrata, sebbene sia necessario prendere debita nota delle informazioni rese disponibili all'interessato prima dell'espressione del consenso. L'uso di caselle di adesione preselezionate non è valido ai sensi del regolamento. Il silenzio o l'inattività da parte dell'interessato, così come il semplice procedere all'uso di un servizio, non possono essere considerati una manifestazione attiva di scelta.

80. Esempio 14: Durante l'installazione di un software, l'applicazione richiede all'interessato di acconsentire a utilizzare segnalazioni di arresto anomalo non anonimizzate per migliorare il software. La richiesta di

consenso è accompagnata da una informativa sulla protezione dei dati a più livelli che fornisce le necessarie informazioni. Selezionando attivamente la casella facoltativa "Acconsento", l'utente è in grado di eseguire validamente una "azione positiva inequivocabile" per acconsentire al trattamento.

81. Il titolare del trattamento deve inoltre fare attenzione al fatto che il consenso non può essere ottenuto tramite la stessa azione con cui si accetta un contratto o le condizioni generali di servizio. L'accettazione globale delle condizioni generali di contratto/servizio non può essere considerata come un'azione positiva inequivocabile ai fini del consenso all'uso dei dati personali. Il regolamento generale sulla protezione dei dati non consente al titolare del trattamento di mettere a disposizione caselle preselezionate o procedure di rinuncia (opt-out) che richiedono un intervento dell'interessato per rifiutare il consenso (ad esempio "caselle di rinuncia")[44].

82. Quando il consenso deve essere prestato a fronte di una richiesta elettronica, quest'ultima non deve interferire *inutilmente* con l'utilizzo del servizio per il quale viene fornito il consenso[45]. Un'azione positiva con cui l'interessato manifesta il proprio consenso può essere necessaria quando una modalità di espressione del consenso meno in violazione e meno invasiva potrebbe determinare ambiguità. Di conseguenza potrebbe essere necessario che, per essere efficace, la richiesta di consenso interrompa in una certa misura l'esperienza d'uso.

83. Tuttavia, nel contesto dei requisiti di cui al regolamento generale sulla protezione dei dati, il titolare del trattamento è libero di sviluppare un flusso di consenso adatto alla propria organizzazione. A questo proposito, le azioni fisiche possono qualificarsi come un'azione positiva inequivocabile in conformità con il regolamento.

84. Il titolare del trattamento dovrebbe progettare meccanismi di consenso che operano in maniera chiara per gli interessati. Il titolare del trattamento deve evitare ambiguità e garantire che l'azione con cui viene espresso il consenso possa essere distinta da altre azioni. La semplice prosecuzione dell'uso normale di un sito web non è pertanto un comportamento dal quale si può dedurre una manifestazione di volontà dell'interessato a prestare il consenso a un trattamento proposto.

85. Esempio 15: Far scorrere una barra su uno schermo, muovere la mano davanti a una telecamera intelligente, ruotare lo smartphone in senso orario o fargli compiere un movimento a otto potrebbero essere opzioni per manifestare il consenso, purché all'interessato siano fornite informazioni inequivocabili e gli sia chiaro che con l'azione in questione acconsente a una richiesta specifica (istruzione esemplificativa: "Se fai scorrere questa barra verso sinistra acconsenti all'uso delle informazioni X per la finalità Y. Ripeti il movimento per confermare"). Il titolare del trattamento deve essere in grado di dimostrare che il consenso è stato

ottenuto in questo modo e l'interessato deve poter revocare il consenso con la stessa facilità con cui lo ha espresso.

86. Esempio 16: In base al considerando 32, azioni quali scorrere un sito o sfogliarne le pagine o azioni analoghe dell'utente non potranno in alcun caso soddisfare il requisito di un'azione positiva inequivocabile: azioni di questo tipo possono essere difficili da distinguere da altre azioni o interazioni dell'utente e quindi non è possibile stabilire che è stato ottenuto un consenso inequivocabile. Inoltre, in un caso del genere, sarà difficile dare all'utente la possibilità di revocare il consenso con la stessa facilità con cui lo ha espresso.

87. Nel contesto digitale molti servizi necessitano di dati personali per funzionare, quindi gli interessati ricevono quotidianamente molteplici richieste di consenso che implicano risposte tramite clic e scorrimenti. Ne può derivare un certo grado di stanchezza a cliccare: se occorre farlo troppe volte, l'effettivo effetto di avvertimento dei meccanismi di consenso diminuisce.

88. Si può quindi verificare la situazione in cui le domande di consenso non vengono più lette, con un conseguente rischio specifico per l'interessato, in quanto in genere viene richiesto il consenso per azioni che in linea di principio sono illecite in assenza di consenso. Il regolamento generale sulla protezione dei dati impone al titolare del trattamento l'obbligo di sviluppare soluzioni per affrontare questo problema.

89. Un esempio spesso citato nel contesto online è l'ottenimento del consenso dell'utente di Internet tramite le impostazioni del browser. Tali impostazioni dovrebbero essere sviluppate in linea con le condizioni per la validità del consenso previste dal regolamento, come ad esempio il fatto che il consenso deve essere granulare per ciascuna delle finalità previste e che le informazioni da fornire per ottenere il consenso devono indicare i titolari del trattamento.

90. In ogni caso, il consenso deve sempre essere ottenuto prima che il titolare del trattamento inizi a trattare i dati personali per i quali è necessario il consenso. Il Gruppo di lavoro Articolo 29 ha costantemente affermato nei suoi pareri che il consenso dovrebbe essere espresso prima dell'avvio dell'attività di trattamento[46]. Sebbene il regolamento non prescriva esplicitamente all'articolo 4, punto 11, che il consenso debba essere manifestato prima dell'attività di trattamento, ciò è chiaramente implicito. La rubrica dell'articolo 6 e il verbo "ha espresso" di cui all'articolo 6, paragrafo 1, lettera a), confermano tale interpretazione. Consegue logicamente dall'articolo 6 e dal considerando 40 che prima di iniziare un trattamento dei dati deve sussistere una base legittima e valida. Pertanto, il consenso dovrebbe essere espresso prima che abbia luogo l'attività di trattamento. In linea di principio può essere sufficiente chiedere il consenso dell'interessato una sola volta. Tuttavia, il titolare del trattamento deve ottenere un nuovo consenso specifico qualora le finalità del trattamento dei dati cambino dopo che è stato ottenuto il consenso o qualora sia prevista una finalità aggiuntiva.

4. OTTENIMENTO DEL CONSENSO ESPLICITO

91. Il consenso esplicito è richiesto in talune circostanze nelle quali emergono gravi rischi per la protezione dei dati e in cui si ritiene quindi appropriato un livello elevato di controllo individuale sui dati personali. Il regolamento generale sulla protezione dei dati richiede il consenso esplicito all'articolo 9 per il trattamento di categorie particolari di dati, all'articolo 49 per i trasferimenti di dati verso paesi terzi od organizzazioni internazionali in assenza di garanzie adeguate[47], e all'articolo 22 per i processi decisionali automatizzati relativi alle persone fisiche, compresa la profilazione[48].

92. In base al regolamento, prerequisito per l'ottenimento di un consenso "conforme" è una "dichiarazione o un'azione positiva inequivocabile". Poiché il requisito del consenso "conforme" nel regolamento è già elevato a un livello superiore rispetto al requisito del consenso di cui alla direttiva 95/46/CE, è necessario chiarire quali sforzi supplementari debba attuare il titolare del trattamento per ottenere il consenso *esplicito* dell'interessato in linea con il regolamento.

93. Il termine *esplicito* si riferisce al modo in cui il consenso è espresso dall'interessato e significa che l'interessato deve fornire una dichiarazione esplicita di consenso. Un modo ovvio per assicurarsi che il consenso sia esplicito consisterebbe nel confermare espressamente il consenso in una dichiarazione scritta. Se del caso, il titolare del trattamento potrebbe assicurarsi che la dichiarazione scritta sia firmata dall'interessato, al fine di dissipare tutti i possibili dubbi e la potenziale mancanza di prove in futuro[49].

94. Tuttavia la dichiarazione firmata non è l'unico modo per ottenere il consenso esplicito e non si può affermare che il regolamento prescriva dichiarazioni scritte e firmate in tutte le circostanze che richiedono un consenso esplicito valido. Ad esempio, nel contesto digitale od online, l'interessato può emettere la dichiarazione richiesta compilando un modulo elettronico, inviando un'e-mail, caricando un documento scansionato con la propria firma oppure utilizzando una firma elettronica. In teoria, anche l'uso di dichiarazioni verbali può essere sufficientemente specifico per ottenere un consenso esplicito valido, tuttavia può essere difficile per il titolare del trattamento dimostrare che tutte le condizioni per la validità del consenso esplicito siano state soddisfatte quando la dichiarazione è stata registrata.

95. Un'organizzazione può anche ottenere il consenso esplicito tramite una conversazione telefonica, a condizione che le informazioni sulla scelta siano corrette, intelligibili e chiare e che venga richiesta una conferma specifica da parte dell'interessato (ad esempio premendo un pulsante o fornendo una conferma verbale).

96. Esempio 17: Il titolare del trattamento può ottenere il consenso esplicito da un visitatore del proprio sito web mettendo a disposizione una schermata di consenso esplicito contenente caselle di controllo "Sì" e "No", a condizione che il testo indichi chiaramente il consenso, ad esempio

con una dicitura del tipo “In questo modo acconsento al trattamento dei miei dati” e non ad esempio tramite una formulazione del tipo “Mi è chiaro che i miei dati saranno trattati”. Va da sé che devono essere soddisfatte le condizioni per il consenso informato e le altre condizioni per la validità del consenso.

97. Esempio 18: Una clinica per chirurgia estetica chiede il consenso esplicito di un paziente al trasferimento della cartella clinica a un esperto per un secondo parere sulla condizione del paziente. La cartella clinica è costituita da un file digitale. Data la natura specifica delle informazioni in questione, la clinica chiede la firma elettronica dell’interessato per ottenere un consenso esplicito valido e per essere in grado di dimostrare che è stato ottenuto detto consenso esplicito[50].

98. Anche la verifica in due fasi del consenso può essere un modo per assicurarsi che il consenso esplicito sia valido. Ad esempio, l’interessato riceve un’e-mail che gli notifica l’intenzione del titolare del trattamento di trattare una cartella contenente dati medici. Il titolare del trattamento spiega nell’e-mail che chiede il consenso all’uso di un insieme specifico di informazioni per una finalità specifica. Se l’interessato acconsente all’utilizzo dei dati, il titolare del trattamento gli chiede una risposta via e-mail contenente la dichiarazione “Acconsento”. Dopo l’invio della risposta, l’interessato riceve un link di verifica da cliccare oppure un messaggio SMS con un codice di verifica, in maniera da confermare il consenso.

99. L’articolo 9, paragrafo 2, non riconosce il trattamento “necessario all’esecuzione di un contratto” come un’eccezione al divieto generale di trattare categorie particolari di dati. Di conseguenza i titolari del trattamento e gli Stati membri che rientrano nel contesto di applicazione di tale circostanza dovrebbero esaminare le eccezioni specifiche di cui all’articolo 9, paragrafo 2, lettere da b) a j). Qualora non si applichi nessuna delle eccezioni da b) a j), l’ottenimento del consenso esplicito in conformità con le condizioni per il consenso valido previste dal regolamento rimane l’unica eccezione lecita possibile per trattare tali dati.

100. Esempio 19: La compagnia aerea Holiday Airways offre un servizio di assistenza di viaggio ai passeggeri che non possono viaggiare senza assistenza, ad esempio a causa di una disabilità. Un cliente prenota un volo da Amsterdam a Budapest e richiede l’assistenza di viaggio per salire a bordo dell’aereo. Holiday Airways richiede al passeggero di fornire informazioni sulle sue condizioni di salute per essere in grado di organizzare i servizi appropriati (ad esempio, una sedia a rotelle a disposizione alla porta di imbarco o un assistente che viaggi con il passeggero da A a B). Holiday Airways richiede il consenso esplicito per trattare i dati sanitari del passeggero allo scopo di organizzare l’assistenza richiesta per il viaggio. I dati trattati sulla base del consenso

devono essere necessari per il servizio richiesto. Inoltre i voli per Budapest sono disponibili anche senza assistenza di viaggio. Si noti che poiché tali dati sono necessari per la prestazione del servizio richiesto, l'articolo 7, paragrafo 4, non si applica.

101. Esempio 20: Un'azienda di successo è specializzata nella fornitura di occhiali da sci e da snowboard su misura e altri tipi di occhiali personalizzati per gli sport all'aria aperta. L'idea è che le persone possano indossare tali occhiali senza dover portare anche gli occhiali da vista. La società riceve ordini presso un punto centrale e consegna prodotti in tutta l'UE a partire da un'unica sede.

102. Per poter fornire i propri prodotti personalizzati ai clienti miopi, tale titolare del trattamento richiede il consenso all'uso delle informazioni sulle condizioni di vista dei clienti. I clienti forniscono i dati sanitari necessari - ad esempio i dati della loro prescrizione - online quando effettuano l'ordine. Senza questi dati non sarebbe possibile fornire gli occhiali personalizzati richiesti. L'azienda offre anche una serie di occhiali con valori correttivi standardizzati. I clienti che non desiderano condividere i dati sanitari possono optare quindi per le versioni standard. Di conseguenza, nel caso di specie, è richiesto un consenso esplicito ai sensi dell'articolo 9 e il consenso può essere considerato come espresso liberamente.

5. CONDIZIONI AGGIUNTIVE PER L'OTTENIMENTO DI UN CONSENSO VALIDO

103. Il regolamento generale sulla protezione dei dati introduce requisiti che impongono al titolare del trattamento di prevedere modalità aggiuntive per garantire che ottiene un consenso valido, lo mantiene e sia in grado di dimostrarne l'esistenza. L'articolo 7 del stabilisce queste condizioni aggiuntive per il consenso valido tramite disposizioni specifiche sulla conservazione di registrazioni del consenso e sul diritto di revocare facilmente il consenso espresso. L'articolo 7 si applica anche al consenso di cui ad altri articoli del regolamento, ad esempio gli articoli 8 e 9. Si riportano in appresso orientamenti sull'ulteriore requisito di dimostrare l'esistenza di un consenso valido e sulla revoca del consenso.

5.1 DIMOSTRAZIONE DEL CONSENSO

104. L'articolo 7, paragrafo 1, prevede in maniera chiara l'obbligo esplicito del titolare del trattamento di dimostrare il consenso dell'interessato. Conformemente a tale articolo, l'onere della prova è a carico del titolare del trattamento.

105. Il considerando 42 afferma: "*Per i trattamenti basati sul consenso dell'inte-*

ressato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento".

106. Il titolare del trattamento è libero di sviluppare metodi propri per rispettare tale disposizione in maniera adatta alle sue attività quotidiane. Allo stesso tempo, l'obbligo in capo al titolare del trattamento di dimostrare l'ottenimento di un consenso valido non dovrebbe di per sé portare a quantità eccessive di trattamenti di dati supplementari. Ciò significa che il titolare del trattamento dovrebbe disporre di dati sufficienti per mostrare un collegamento al trattamento (ossia per fornire la prova che è stato ottenuto il consenso) ma non dovrebbe raccogliere più informazioni di quanto necessario.

107. Spetta al titolare del trattamento dimostrare che è stato ottenuto un consenso valido dall'interessato. Il regolamento non prescrive esattamente come ciò debba avvenire. Tuttavia, il titolare del trattamento deve essere in grado di dimostrare che l'interessato nel caso specifico ha espresso il proprio consenso. Fintantoché dura l'attività di trattamento dei dati in questione, sussiste l'obbligo di dimostrare l'esistenza del consenso. Al termine dell'attività di trattamento, la prova del consenso deve essere conservata non più di quanto strettamente necessario per adempiere ad obblighi giuridici o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, in conformità con l'articolo 17, paragrafo 3, lettere b) ed e).

108. Ad esempio, il titolare del trattamento può tenere una registrazione delle dichiarazioni di consenso ricevute onde poter dimostrare come e quando è stato ottenuto il consenso, e rendere dimostrabili le informazioni fornite all'interessato al momento dell'espressione del consenso. Il titolare del trattamento deve anche essere in grado di dimostrare che l'interessato è stato informato e che la propria procedura ha soddisfatto tutti i criteri pertinenti per la validità del consenso. La logica alla base di tale obbligo è che il titolare del trattamento deve essere responsabilizzato in relazione all'ottenimento di un consenso valido dell'interessato e ai meccanismi di consenso che ha messo in atto. Ad esempio, in un contesto online, il titolare del trattamento può conservare informazioni sulla sessione in cui è stato espresso il consenso, unitamente alla documentazione della procedura di consenso al momento della sessione, oltre a una copia delle informazioni presentate all'interessato in quel momento. Non sarebbe sufficiente fare semplicemente riferimento a una corretta configurazione del sito web.

109. Esempio 21: Un ospedale istituisce un programma di ricerca scientifica per il quale sono necessarie cartelle cliniche odontoiatriche di pazienti. I partecipanti sono selezionati tramite telefonate a pazienti che hanno volontariamente accettato di essere inseriti in un elenco di candidati che possono essere contattati a tale fine. Il titolare del trattamento chiede il consenso esplicito degli interessati all'uso della loro cartella clinica odontoiatrica. Il consenso viene ottenuto durante

una telefonata, registrando una dichiarazione verbale dell'interessato nella quale quest'ultimo conferma di acconsentire all'uso dei suoi dati per le finalità del programma.

110. Il regolamento non specifica alcun termine per la durata del consenso. Questa dipenderà dal contesto, dalla portata del consenso originale e dalle aspettative dell'interessato. Se i trattamenti cambiano o si evolvono in maniera considerevole, il consenso originale non è più valido e occorrerà un nuovo consenso.

111. Come migliore prassi il Comitato raccomanda di aggiornare il consenso a intervalli appropriati. Fornire nuovamente tutte le informazioni contribuisce a garantire che l'interessato rimanga ben informato su come vengono utilizzati i suoi dati e su come può esercitare i suoi diritti[51].

5.2 REVOCA DEL CONSENSO

112. Il regolamento generale sulla protezione dei dati dà ampio rilievo alla revoca del consenso. Le disposizioni e i considerando relativi alla revoca del consenso possono considerarsi una codificazione dell'interpretazione data al riguardo nei pareri del Gruppo di lavoro Articolo 29[52].

113. L'articolo 7, paragrafo 3, prescrive che il titolare del trattamento deve garantire che l'interessato possa revocare il consenso in qualsiasi momento con la stessa facilità con cui lo ha espresso. Il regolamento non dispone che l'espressione e la revoca del consenso debbano avvenire sempre allo stesso modo.

114. Tuttavia, quando il consenso viene prestato per via elettronica con un solo clic di mouse, un solo scorrimento o premendo un tasto, l'interessato deve, in pratica, poterlo revocare con altrettanta facilità. Se il consenso è espresso attraverso un'interfaccia utente specifica di servizio (ad esempio un sito web, un'applicazione, un account protetto, l'interfaccia di un dispositivo IoT oppure posta elettronica), è indubbio che l'interessato deve poterlo revocare tramite la medesima interfaccia elettronica, poiché il passaggio a un'altra interfaccia per la sola revoca richiederebbe uno sforzo eccessivo. Inoltre, l'interessato dovrebbe poter revocare il consenso senza subire pregiudizio. Ciò significa, tra l'altro, che il titolare del trattamento deve consentire la revoca senza spese o senza abbassare i livelli del servizio[53].

115. Esempio 22: Un festival musicale vende biglietti tramite un agente di vendita di biglietti online. All'atto della vendita del biglietto viene richiesto il consenso all'uso dei dettagli di contatto per finalità di marketing. Per acconsentire o meno a tale finalità, il cliente può cliccare su "Sì" oppure su "No". Il titolare del trattamento informa il cliente che

può revocare il consenso contattando gratuitamente un call center nei giorni lavorativi tra le 8:00 e le 17:00. Il titolare del trattamento di questo esempio non rispetta l'articolo 7, paragrafo 3, del regolamento. Telefonare durante l'orario di lavoro per revocare il consenso è più oneroso rispetto a un clic di mouse per prestare il consenso attraverso il venditore di biglietti online, che è aperto 24 ore al giorno, 7 giorni la settimana.

116. In base al regolamento il requisito della facilità della revoca è un elemento necessario del consenso valido. Se il diritto di revoca non soddisfa i requisiti del regolamento, il meccanismo di consenso del titolare del trattamento non è conforme al regolamento. Come menzionato nella sezione 3.1 sulla condizione del consenso *informato*, a norma dell'articolo 7, paragrafo 3, del regolamento il titolare del trattamento deve informare l'interessato del diritto di revoca prima che quest'ultimo presti effettivamente il consenso. Inoltre, nel contesto dell'obbligo di trasparenza, il titolare del trattamento deve informare l'interessato sulle modalità di esercizio dei suoi diritti[54].

117. Di norma, se il consenso viene revocato, tutti i trattamenti dei dati basati sul consenso avvenuti prima della revoca (e in conformità con il regolamento) rimangono leciti, tuttavia il titolare del trattamento deve interrompere le attività di trattamento interessate. Qualora non sussista un'altra base legittima per il trattamento (ad esempio l'ulteriore archiviazione) dei dati, questi dovrebbero essere cancellati dal titolare del trattamento[55].

118. Come già accennato, prima di raccogliere i dati è molto importante che il titolare del trattamento valuti le finalità per le quali i dati sono effettivamente trattati e le basi legittime del trattamento. Spesso le aziende hanno bisogno di dati personali per diverse finalità e il trattamento si basa su più basi legittime, ad esempio il trattamento di dati dei clienti può basarsi su un contratto e sul consenso. Di conseguenza, la revoca del consenso non implica che il titolare del trattamento deve cancellare i dati trattati per una finalità che si basa sull'esecuzione del contratto stipulato con l'interessato. Il titolare del trattamento dovrebbe pertanto precisare chiaramente sin dall'inizio la finalità che si applica a ciascun dato e le basi legittime del trattamento.

119. Il titolare del trattamento deve cancellare i dati trattati sulla base del consenso non appena questo viene revocato, supponendo che non vi siano altre finalità che giustificano l'ulteriore conservazione[56]. Oltre a questa situazione, prevista dall'articolo 17, paragrafo 1, lettera b)[57], l'interessato può chiedere la cancellazione di altri dati che lo riguardano trattati sulla base di un'altra base legittima, ad esempio l'articolo 6, paragrafo 1, lettera b). Il titolare del trattamento è tenuto a valutare se la prosecuzione del trattamento dei dati in questione sia appropriata, anche in assenza di una richiesta di cancellazione da parte dell'interessato[58].

120. In caso di revoca del consenso, il titolare del trattamento, se vuole continuare a trattare i dati personali in base a un'altra base legittima, non può passare tacitamente dal consenso (che è stato revocato) all'altra base legittima. Qualsiasi modifica della base legittima del trattamento deve essere notificata all'interessato in conformità ai requisiti di informazione di cui agli articoli 13 e 14, nonché al principio generale di trasparenza.

6. INTERAZIONE TRA IL CONSENSO E ALTRE BASI LEGITTIME DI CUI ALL'ARTICOLO 6 DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

121. L'articolo 6 stabilisce le condizioni per la liceità del trattamento dei dati personali ed elenca sei basi legittime su cui il titolare del trattamento può fondarsi. L'applicazione di una di queste sei basi deve essere stabilita prima di procedere al trattamento e in relazione a una finalità specifica[59].

122. È importante osservare che, se sceglie di basarsi sul consenso per ogni parte del trattamento, il titolare del trattamento deve essere preparato a rispettare tale scelta e interrompere la parte del trattamento in caso di revoca del consenso. Comunicare che i dati saranno trattati sulla base del consenso mentre in realtà si fa affidamento su un'altra base legittima sarebbe fondamentalmente scorretto nei confronti dell'interessato.

123. In altre parole, il titolare del trattamento non può passare dal consenso ad altre basi legittime. Ad esempio non può ricorrere retroattivamente alla base dell'interesse legittimo in caso di problemi di validità del consenso. Poiché ha l'obbligo di comunicare la base legittima al momento della raccolta dei dati personali, il titolare del trattamento deve aver deciso la base legittima prima della raccolta dei dati.

7. SETTORI SPECIFICI DI INTERESSE NEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

7.1 MINORI (ARTICOLO 8)

124. Rispetto alla direttiva attuale, il regolamento generale sulla protezione dei dati crea un ulteriore livello di protezione per il trattamento dei dati personali delle persone fisiche vulnerabili, in particolare i minori. L'articolo 8 introduce obblighi supplementari per garantire una maggiore protezione dei dati dei minori in relazione ai servizi della società dell'informazione. I motivi di tale protezione rafforzata sono specificati nel considerando 38: "*I minori [...] possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali [...]*". Sempre al considerando 38 si afferma che "*[t]ale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili*

di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore". La precisazione "in particolare" indica che la protezione specifica non si limita al marketing o alla profilazione, ma si estende alla più ampia "raccolta di dati personali relativi ai minori".

125. L'articolo 8, paragrafo 1, stabilisce che laddove si applichi il consenso, per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui il consenso è prestato o autorizzato dal titolare della responsabilità genitoriale[60]. Per quanto concerne il limite di età per il consenso valido, il regolamento offre flessibilità, in quanto gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

126. Come menzionato nella sezione 3.1. sul consenso informato, le informazioni fornite dal titolare del trattamento devono essere comprensibili per il pubblico al quale sono destinate, con particolare attenzione alla posizione dei minori. Per ottenere il "consenso informato" di un minore, il titolare del trattamento deve spiegare in un linguaggio chiaro e semplice, comprensibile per i minori, come intende trattare i dati raccolti[61]. Se spetta al genitore prestare il consenso, può essere necessario fornire un insieme di informazioni che consentano agli adulti di prendere una decisione informata.

127. Da quanto precede risulta evidente che l'articolo 8 si applica esclusivamente quando sono soddisfatte le seguenti condizioni:

- il trattamento è correlato all'offerta diretta di servizi della società dell'informazione ai minori[62,63];
- il trattamento è basato sul consenso.

7.1.1. SERVIZIO DELLA SOCIETÀ DELL'INFORMAZIONE

128. Al fine di determinare la portata dell'espressione "servizio della società dell'informazione", il regolamento generale sulla protezione dei dati, all'articolo 4, punto 25, fa riferimento alla direttiva (UE) 2015/1535.

129. Per valutare la portata di tale definizione, il Comitato fa riferimento anche alla giurisprudenza della Corte di giustizia[64]. La Corte di giustizia ha affermato che la nozione di *servizi della società dell'informazione* interessa contratti e altri servizi conclusi o trasmessi online. Laddove un servizio presenti due componenti economicamente indipendenti, una delle quali è la componente online (ad esempio l'offerta e l'accettazione di un'offerta nel contesto della conclusione di un contratto, o le informazioni relative a prodotti o servizi, comprese le attività di marketing) e l'altra è la consegna fisica o la distribuzione di merci, la prima rientra nella definizione di servizio della società dell'informazione, mentre la seconda no. La

consegna online di un servizio rientrerebbe nell'espressione *servizio della società dell'informazione* di cui all'articolo 8 del regolamento generale sulla protezione dei dati.

7.1.2 FORNITI DIRETTAMENTE A UN MINORE

130. La precisazione "offerta diretta [...] ai minori" indica che l'articolo 8 si applica ad alcuni ma non a tutti i servizi della società dell'informazione. A tale riguardo, se un prestatore di servizi della società dell'informazione chiarisce ai potenziali utenti che il servizio è offerto esclusivamente a persone aventi almeno 18 anni, e ciò non è smentito da altri elementi (come il contenuto del sito o piani di marketing), allora il servizio non sarà considerato fornito direttamente a un minore e l'articolo 8 non si applicherà.

7.1.3. ETÀ

131. Il regolamento specifica che "*[g]li Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni*". Nel tenere conto del pubblico destinatario dei suoi servizi, il titolare del trattamento deve tenere presenti le diverse leggi nazionali. In particolare, il titolare del trattamento che fornisce un servizio transfrontaliero non può sempre fare affidamento sul solo rispetto della legge dello Stato membro in cui ha lo stabilimento principale, perché potrebbe dover rispettare le leggi nazionali di ciascuno Stato membro in cui offre i servizi della società dell'informazione, a seconda che lo Stato membro scelga di usare come criterio di legge il luogo dello stabilimento principale del titolare del trattamento oppure il luogo di residenza dell'interessato. Nello scegliere il criterio da usare gli Stati membri devono considerare innanzitutto l'interesse superiore del minore. Il Comitato incoraggia gli Stati membri a cercare una soluzione armonizzata.

132. Nel fornire servizi della società dell'informazione ai minori sulla base del consenso, il titolare del trattamento dovrà compiere ogni ragionevole sforzo per verificare che l'utente abbia raggiunto l'età del consenso digitale, e le misure dovrebbero essere proporzionate alla natura e ai rischi delle attività di trattamento.

133. Se l'utente afferma di aver raggiunto l'età del consenso digitale, il titolare del trattamento può effettuare controlli appropriati per verificare la veridicità della dichiarazione. Sebbene il regolamento non richieda esplicitamente di intraprendere sforzi ragionevoli per verificare l'età, tale necessità è implicita, poiché se un minore presta il consenso senza avere l'età sufficiente per prestare un consenso valido per proprio conto il trattamento dei dati sarà illecito.

134. Se l'utente dichiara di avere un'età inferiore a quella del consenso digitale, il titolare del trattamento può accettare tale dichiarazione senza ulteriori verifiche, ma dovrà ottenere l'autorizzazione dei genitori e verificare che la persona che esprime il consenso sia titolare della responsabilità genitoriale.

135. La verifica dell'età non deve comportare un eccessivo trattamento di dati. Il meccanismo scelto per verificare l'età dell'interessato dovrebbe prevedere una valutazione del rischio del trattamento proposto. In alcune situazioni a basso rischio, potrebbe essere adeguato richiedere al nuovo abbonato al servizio di rivelare il proprio anno di nascita oppure di compilare un modulo in cui dichiara di (non) essere un minore[65]. Qualora dovessero sorgere dubbi, il titolare del trattamento dovrebbe riesaminare i meccanismi di verifica dell'età nel caso di specie e valutare se siano necessari controlli alternativi[66].

7.1.4 CONSENSO DEL MINORE E RESPONSABILITÀ GENITORIALE

136. Per quanto riguarda l'autorizzazione del titolare della responsabilità genitoriale, il regolamento non prevede modalità pratiche per raccogliere il consenso del genitore o per stabilire che qualcuno è autorizzato a prestare il consenso[67]. Di conseguenza il Comitato raccomanda l'adozione di un approccio proporzionato, in linea con l'articolo 8, paragrafo 2, e l'articolo 5, paragrafo 1, lettera c), del regolamento (minimizzazione dei dati). Un approccio proporzionato potrebbe essere quello di concentrarsi sull'ottenimento di una quantità limitata di informazioni, ad esempio i dettagli di contatto di un genitore o del tutore.

137. La ragionevolezza degli sforzi, in termini di verifica tanto che l'utente abbia l'età sufficiente per esprimere il consenso quanto che la persona che esprime il consenso a nome del minore sia il titolare della responsabilità genitoriale, può dipendere dai rischi inerenti al trattamento e dalla tecnologia disponibile. Nei casi a basso rischio, può essere sufficiente la verifica della responsabilità genitoriale a mezzo posta elettronica. Viceversa, nei casi ad alto rischio, può essere opportuno chiedere ulteriori prove affinché il titolare del trattamento sia in grado di verificare e conservare le informazioni di cui all'articolo 7, paragrafo 1[68]. I servizi di verifica di terzi fidati possono offrire soluzioni che riducono al minimo la quantità di dati personali che il titolare del trattamento deve trattare autonomamente.

138. Esempio 23: Una piattaforma di gioco online vuole assicurarsi che i clienti minorenni si abbonino ai servizi esclusivamente con il consenso dei genitori o tutori. Il titolare del trattamento segue questi passaggi:

139. passaggio 1: chiede all'utente di indicare se ha meno o più di 16 anni (o dell'età alternativa per il consenso digitale). Se l'utente dichiara di

avere un'età inferiore a quella per il consenso digitale:

140. passaggio 2: il servizio informa il minore della necessità che un genitore o il tutore acconsenta o autorizzi il trattamento prima che venga erogato il servizio. All'utente viene quindi richiesto di rivelare l'indirizzo di posta elettronica di un genitore o del tutore;

141. passaggio 3: il servizio contatta il genitore o il tutore e ne ottiene il consenso al trattamento tramite posta elettronica e adotta misure ragionevoli per ottenere la conferma che l'adulto abbia la responsabilità genitoriale;

142. passaggio 4: in caso di reclami, la piattaforma adotta ulteriori provvedimenti per verificare l'età dell'abbonato.

143. Se soddisfa gli altri requisiti del consenso, la piattaforma può soddisfare i criteri supplementari di cui all'articolo 8 del regolamento seguendo questi passaggi.

144. L'esempio mostra che il titolare del trattamento può mettersi in una posizione tale da dimostrare che sono stati compiuti sforzi ragionevoli per garantire che è stato ottenuto un consenso valido in relazione ai servizi forniti a un minore. L'articolo 8, paragrafo 2, aggiunge in particolare che "*[i]l titolare del trattamento si adopera in ogni modo ragionevole per verificare che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili*".

145. Spetta al titolare del trattamento stabilire quali misure siano appropriate in un caso specifico. Di norma, il titolare del trattamento dovrebbe evitare soluzioni di verifica che implichino una raccolta eccessiva di dati personali.

146. Il Comitato riconosce che in determinati casi la verifica è difficile, ad esempio se il minore che presta il consenso non ha ancora lasciato un'"impronta di identità" o se la responsabilità genitoriale non è facilmente verificabile. Tale aspetto può essere preso in considerazione nel decidere quali sforzi siano ragionevoli, tuttavia ci si aspetta anche che il titolare del trattamento tenga sotto costante controllo i suoi processi e la tecnologia disponibile.

147. Per quanto riguarda l'autonomia dell'interessato a manifestare il consenso al trattamento dei dati personali e il pieno controllo sul trattamento, nel momento in cui raggiunge l'età del consenso digitale l'interessato può confermare, modificare o revocare il consenso prestato o autorizzato dal titolare della responsabilità genitoriale.

148. In pratica, ciò significa che se il minore non intraprende alcuna azione, il consenso prestato o autorizzato dal titolare della responsabilità genitoriale in relazione al trattamento dei dati personali forniti prima dell'età del consenso digitale rimarrà un presupposto valido per il trattamento.

149. Una volta raggiunta l'età del consenso digitale, il minore avrà la possibi-

lità di revocare il consenso, in linea con l'articolo 7, paragrafo 3. In conformità con i principi di correttezza e responsabilizzazione, il titolare del trattamento deve informare il minore di questa possibilità[69].

150. È importante sottolineare che, ai sensi del considerando 38, il consenso di un genitore o del tutore non è richiesto nel contesto di servizi di prevenzione o consulenza offerti direttamente al minore. Ad esempio, per i servizi di protezione dei minori offerti online ai minori tramite un servizio di chat non occorre la previa autorizzazione dei genitori.

151. Infine, il regolamento prevede che le norme relative ai requisiti di autorizzazione genitoriale nei confronti dei minori non pregiudicano "le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore". Di conseguenza i requisiti per la validità del consenso all'uso dei dati relativi a minori rientrano in un quadro giuridico da considerarsi distinto dal diritto contrattuale nazionale. Le presenti linee guida non affrontano pertanto la questione se sia lecito o meno per un minore concludere contratti online. Entrambi i regimi giuridici possono essere applicati simultaneamente e l'ambito di applicazione del regolamento generale sulla protezione dei dati non include l'armonizzazione delle disposizioni nazionali di diritto contrattuale.

7.2 RICERCA SCIENTIFICA

152. La definizione di finalità di ricerca scientifica ha implicazioni sostanziali per la gamma di attività di trattamento di dati che un titolare del trattamento può intraprendere. L'espressione "*ricerca scientifica*" non è definita nel regolamento. Il considerando 159 afferma: "*[...] Nell'ambito del presente regolamento, il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato. [...]*", tuttavia il Comitato ritiene che tale nozione non possa essere estesa oltre il suo significato comune e che per "*ricerca scientifica*" in questo contesto si intenda un progetto di ricerca istituito in conformità con le pertinenti norme metodologiche e deontologiche settoriali, in linea con le buone prassi.

153. Quando il consenso costituisce la base legittima per condurre ricerche in conformità con il regolamento, tale consenso all'uso dei dati personali dovrebbe essere distinto dagli altri requisiti del consenso che fungono da norme deontologiche od obbligo procedurale. Un esempio di obbligo procedurale, in cui il trattamento si basa non sul consenso ma su un'altra base giuridica, figura nel regolamento sulla sperimentazione clinica. Nel contesto del diritto in materia di protezione dei dati, quest'ultima forma di consenso potrebbe essere considerata una garanzia aggiuntiva[70]. Allo stesso tempo, il regolamento generale sulla protezione dei dati non limita l'applicazione dell'articolo 6 al solo consenso, per quanto riguarda il trattamento di dati per fini di ricerca. Fintantoché sussistono garanzie adeguate, quali i requisiti di cui all'articolo 89, paragrafo 1, e il tratta-

mento è corretto, lecito, trasparente e conforme alle norme sulla minimizzazione dei dati e ai diritti individuali, potrebbero essere disponibili altre basi legittime quali l'articolo 6, paragrafo 1, lettera e) o f)[71]. Ciò vale anche per le categorie particolari di dati ai sensi della deroga di cui all'articolo 9, paragrafo 2, lettera j)[72].

154. Il considerando 33 sembra consentire una certa flessibilità al grado di specificazione e granularità del consenso nel contesto della ricerca scientifica. Il considerando 33 afferma: "*In molti casi non è possibile individuare pienamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica. Gli interessati dovrebbero avere la possibilità di prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista*".

155. In primo luogo, va osservato che il considerando 33 non inficia gli obblighi relativi al requisito del consenso specifico. Ciò significa che, in linea di principio, i progetti di ricerca scientifica possono includere dati personali sulla base del consenso soltanto se hanno una finalità ben descritta. Nei casi in cui le finalità del trattamento dei dati nell'ambito di un progetto di ricerca scientifica non possono essere specificate in via preliminare, il considerando 33 consente in via eccezionale che la finalità possa essere descritta a un livello più generale.

156. Tenuto conto delle condizioni rigorose stabilite dall'articolo 9 in merito al trattamento di categorie particolari di dati, il Comitato rileva che quando categorie particolari di dati vengono trattate sulla base del consenso esplicito, l'applicazione dell'approccio flessibile di cui al considerando 33 sarà soggetta a un'interpretazione più rigorosa e richiede un elevato livello di controllo.

157. Considerato nel suo insieme, il regolamento generale sulla protezione dei dati non può essere interpretato in maniera tale da consentire al titolare del trattamento di aggirare il principio chiave della specificazione delle finalità per le quali viene richiesto il consenso dell'interessato.

158. Quando non è possibile specificare appieno le finalità della ricerca, il titolare del trattamento deve cercare altri modi per garantire il rispetto dell'essenza dei requisiti del consenso, ad esempio permettendo agli interessati di acconsentire a una finalità di ricerca in termini più generali e a fasi specifiche di un progetto di ricerca che si sa già sin dall'inizio avranno luogo. Mano a mano che la ricerca avanza, sarà quindi possibile ottenere il consenso per le fasi successive del progetto prima dell'inizio della fase corrispondente. Tuttavia, tale consenso dovrebbe comunque essere in linea con le norme deontologiche applicabili alla ricerca scientifica.

159. Inoltre, il titolare del trattamento può applicare ulteriori garanzie in questi casi. L'articolo 89, paragrafo 1, ad esempio, sottolinea la necessità di

prevedere garanzie nelle attività di trattamento di dati per fini di ricerca scientifica o storica o per fini statistici. Tali finalità "*[sono] soggett[e] a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento*". Come possibili garanzie si menzionano la minimizzazione dei dati, l'anonimizzazione e la sicurezza dei dati[73]. L'anonimizzazione rappresenta la soluzione preferita non appena la finalità della ricerca possa essere conseguita senza il trattamento di dati personali.

160. La trasparenza è un'ulteriore garanzia quando le circostanze della ricerca non consentono un consenso specifico. La mancanza di specificazione della finalità può essere compensata dalla fornitura periodica, da parte del titolare del trattamento, di informazioni sullo sviluppo della finalità durante l'avanzamento del progetto di ricerca, in maniera tale che, nel tempo, il consenso sia il più specifico possibile. In tal modo l'interessato ha quanto meno una conoscenza di base dello stato di avanzamento, che gli consente di valutare se esercitare o meno, ad esempio, il diritto di revoca del consenso ai sensi dell'articolo 7, paragrafo 3[74].

161. Anche la messa a disposizione di un piano di ricerca esaustivo al quale gli interessati possano fare riferimento prima di esprimere il loro consenso potrebbe contribuire a compensare una mancanza di specificazione delle finalità. Il piano di ricerca dovrebbe specificare nella maniera più chiara possib[75]ile i quesiti che la ricerca si pone e i metodi di lavoro previsti. Il piano di ricerca potrebbe altresì contribuire al rispetto dell'articolo 7, paragrafo 1, in quanto, per poter dimostrare che il consenso è valido, il titolare del trattamento è tenuto a dimostrare quali informazioni erano disponibili agli interessati al momento dell'espressione del consenso.

162. È importante ricordare che quando il consenso costituisce la base legittima del trattamento, l'interessato deve avere la possibilità di revocarlo. Il Comitato rileva che la revoca del consenso potrebbe compromettere taluni tipi di ricerca scientifica che richiedono dati che possano essere collegati a persone fisiche, tuttavia il regolamento è chiaro nello stabilire che il consenso può essere revocato e che il titolare del trattamento deve tenerne conto: non vi è alcuna esenzione a questo requisito per la ricerca scientifica. Se riceve una richiesta di revoca, il titolare del trattamento deve, in linea di principio, cancellare immediatamente i dati personali se vuole continuare a utilizzare i dati per le finalità della ricerca[76].

7.3 DIRITTI DELL'INTERESSATO

163. Se l'attività di trattamento di dati si basa sul consenso, i diritti dell'interessato subiscono alcune ripercussioni: l'interessato può avere il diritto alla portabilità dei dati (articolo 20), ma non il diritto di opposizione (articolo 21), sebbene il diritto di revocare il consenso in qualsiasi momento possa portare a un esito analogo.

164. Gli articoli da 16 a 20 del regolamento generale sulla protezione dei dati

indicano che (quando il trattamento dei dati è basato sul consenso) l'interessato ha il diritto alla cancellazione, in caso di revoca del consenso, e i diritti di limitazione del trattamento, rettifica e accesso[77].

8. CONSENSO OTTENUTO A NORMA DELLA DIRETTIVA 95/46/CE

165. I titolari del trattamento che attualmente trattano dati sulla base del consenso conformemente alla normativa nazionale in materia di protezione dei dati non sono automaticamente tenuti a rinnovare completamente tutte le relazioni di consenso con gli interessati in preparazione dell'entrata in vigore del regolamento generale sulla protezione dei dati. Il consenso ottenuto continua ad essere valido nella misura in cui è in linea con le condizioni stabilite nel regolamento generale sulla protezione dei dati.

166. È importante che prima del 25 maggio 2018 i titolari del trattamento rivedano in maniera approfondita i processi di lavoro e le registrazioni correnti, al fine di accertarsi che i consensi in essere soddisfino quanto previsto dal regolamento generale sulla protezione dei dati (cfr. il considerando 171 del regolamento generale sulla protezione dei dati)[78]. In pratica, il regolamento generale sulla protezione dei dati fissa prescrizioni più rigorose riguardo all'attuazione di meccanismi di consenso e introduce nuovi requisiti che impongono ai titolari del trattamento di modificare i meccanismi di consenso, non di riscrivere soltanto le politiche in materia di protezione dei dati[79].

167. Ad esempio, poiché il regolamento impone al titolare del trattamento di essere in grado di dimostrare che ha ottenuto un consenso valido, tutti i presunti consensi dei quali non viene conservato alcun riferimento si considereranno automaticamente al di sotto del livello di consenso fissato dal regolamento e dovranno quindi essere rinnovati. Analogamente, poiché il regolamento richiede una "dichiarazione o un'azione positiva inequivocabile", tutti i presunti consensi basati su una forma di azione più implicita dell'interessato (ad esempio una casella di adesione preselezionata) non saranno conformi al livello di consenso stabilito dal regolamento.

168. Inoltre, per poter dimostrare l'ottenimento del consenso o fornire indicazioni più granulari sulle volontà dell'interessato, il titolare del trattamento potrebbe dover effettuare un riesame delle operazioni e dei sistemi informativi. Devono essere disponibili meccanismi che consentano agli interessati di revocare facilmente il consenso e devono essere fornite informazioni su come revocare il consenso. Se le procedure esistenti per l'ottenimento e la gestione del consenso non soddisfano i livelli previsti dal regolamento, il titolare del trattamento dovrà ottenere un nuovo consenso conforme al regolamento.

169. D'altro canto, poiché non tutti gli elementi indicati negli articoli 13 e 14

devono sempre essere presenti come condizione per un consenso informato, gli obblighi di informazione estesa ai sensi del regolamento non si oppongono necessariamente alla continuità del consenso prestato prima dell'entrata in vigore del regolamento (cfr. la precedente pagina 15). La direttiva 95/46/CE non prevedeva alcun obbligo di informare gli interessati in merito alla base del trattamento.

170. Qualora ritenga che il consenso ottenuto in base alla vecchia normativa non rispetti le norme per il consenso fissate dal regolamento, il titolare del trattamento deve agire per conformarvisi, ad esempio mediante il rinnovo del consenso in una maniera conforme al regolamento. Ai sensi del regolamento non è possibile passare da una base legittima a un'altra. Se il titolare del trattamento non è in grado di rinnovare il consenso in maniera conforme né è in grado, come circostanza una tantum, di conformarsi al regolamento basando il trattamento dei dati su una base legittima diversa garantendo nel contempo che la prosecuzione del trattamento corrisponda ai principi di correttezza e responsabilizzazione, le attività di trattamento devono essere interrotte. In ogni caso, il titolare del trattamento deve rispettare i principi di un trattamento lecito, corretto e trasparente.

NOTE

[1] Nel presente documento, i riferimenti agli "Stati membri" sono da intendersi come riferimenti agli "Stati membri del SEE".

[2] L'articolo 9 del regolamento generale sulla protezione dei dati fornisce un elenco di possibili esenzioni al divieto di trattamento di categorie particolari di dati. Una delle esenzioni elencate è il consenso esplicito dell'interessato all'uso di tali dati.

[3] Cfr. anche il parere 15/2011 del Gruppo di lavoro Articolo 29 sulla definizione di consenso (WP 187), pagine 6-8 e/o il parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE (WP 217), pagg. 9, 10, 13 e 14.

[4] In particolare il parere 15/2011 sulla definizione di consenso (WP 187).

[5] Parere 15/2011 sulla definizione di consenso (WP 187), pag. 9.

[6] Cfr. anche il parere 15/2011 sulla definizione di consenso (WP 187) e l'articolo 5 del regolamento generale sulla protezione dei dati.

[7] Ai sensi dell'articolo 9 della proposta di regolamento sulla vita privata e le comunicazioni elettroniche, si applicano la definizione e le condizioni per il consenso di cui all'articolo 4, punto 11, e all'articolo 7, del regolamento generale sulla protezione dei dati.

[8] Cfr. la dichiarazione del Comitato in materia di ePrivacy del 25 maggio 2018 e la dichiarazione del Comitato n. 3/2019 su un regolamento relativo all'e- privacy.

[9] Cfr. l'articolo 94 del regolamento generale sulla protezione dei dati.

[10] Il consenso, definito nella direttiva 95/46/CE come *"qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento"*, deve essere *"manifestato in maniera inequivocabile"* in maniera da rendere legittimo il trattamento dei dati personali (articolo 7, lettera a), della direttiva 95/46/CE). Cfr. il parere 15/2011 del Gruppo di lavoro Articolo 29 sulla definizione di consenso (WP 187), per esempi sull'adeguatezza del consenso come base legittima. In tale parere, il Gruppo di lavoro Articolo 29 ha fornito linee guida atte a distinguere il caso in cui il consenso costituisca una base lecita appropriata rispetto ai casi in cui è sufficiente fare affidamento su motivi di interesse legittimo (magari offrendo un'opportunità di rinuncia, "opt-out") o sarebbe raccomandabile fondare il trattamento su un rapporto contrattuale. Cfr. anche il parere 6/2014 del Gruppo di lavoro Articolo 29, sezione III.1.2, pag. 17 e successive. Il consenso esplicito è anche una delle esenzioni al divieto di trattamento di categorie particolari di dati: cfr. l'articolo 9 del regolamento generale sulla protezione dei dati.

[11] Per orientamenti in merito alle attività di trattamento in corso basate sul consenso di cui alla direttiva 95/46, cfr. il capitolo 7 del presente documento e il considerando 171 del regolamento generale sulla protezione dei dati.

[12] In svariati pareri il Gruppo di lavoro Articolo 29 ha esaminato i limiti del consenso in situazioni in cui non sia possibile esprimerlo liberamente. Ciò è avvenuto in particolare nei seguenti documenti del Gruppo: parere 15/2011 sulla definizione di consenso (WP 187), documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (WP 131), parere 8/2001 sul trattamento dei dati personali nel contesto lavorativo (WP 48) e "Second opinion 4/2009 on processing of data by the World Anti-Doping Agency (WADA) (International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations" [Secondo parere 4/2009 sul trattamento dei dati da parte dell'Agenzia mondiale antidoping (AMA) - norma internazionale per la tutela della vita privata e delle informazioni personali, sulle relative disposizioni del codice AMA e sulla altre questioni relative alla tutela della vita privata nel contesto della lotta contro il doping nello sport da parte dell'AMA e delle organizzazioni (nazionali) antidoping] (WP 162).

[13] Cfr. il parere 15/2011 sulla definizione di consenso (WP 187), pag. 13.

[14] Cfr. i considerando 42 e 43 del regolamento generale sulla protezione dei dati e il parere 15/2011 del Gruppo di lavoro Articolo 29 sulla definizione di consenso, adottato il 13 luglio 2011 (WP 187), pag. 13.

[15] Il considerando 43 del regolamento generale sulla protezione dei dati afferma: "*Per*

assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. (...)".

[16] Cfr. l'articolo 6 del regolamento generale sulla protezione dei dati, in particolare il paragrafo 1, lettere c) ed e).

[17] Ai fini di questo esempio, con "scuola pubblica" si intende una scuola finanziata con fondi pubblici o qualsiasi struttura educativa che si qualifica come un'autorità pubblica o un ente pubblico ai sensi della legislazione nazionale.

[18] Cfr. anche l'articolo 88 del regolamento generale sulla protezione dei dati, nel quale si sottolinea la necessità di tutelare gli interessi specifici dei dipendenti e si crea una possibilità di deroga nel diritto degli Stati membri. Cfr. anche il considerando 155.

[19] Cfr. il parere 15/2011 sulla definizione di consenso (WP 187), pagg. 13-15; parere 8/2001 sul trattamento dei dati personali nel contesto lavorativo (WP 48), capitolo 10; documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro (WP 55), punto 4.2; e parere 2/2017 sul trattamento dei dati sul posto di lavoro (WP 249), punto 6.2.

[20] Cfr. il parere 2/2017 sul trattamento dei dati sul posto di lavoro, pagg. 6-7.

[21] Cfr. anche il parere 2/2017 sul trattamento dei dati sul lavoro (WP 249), punto 6.2.

[22] L'articolo 7, paragrafo 4, del regolamento generale sulla protezione dei dati recita: *"Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto". Cfr. anche il considerando 43 dello stesso regolamento, che afferma: "[...] Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione".*

[23] Per maggiori informazioni ed esempi, cfr. parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, adottato dal Gruppo di lavoro Articolo 29 il 9 aprile 2014, pagg. 19-20. (WP 217).

[24] La base legittima appropriata in tal caso potrebbe infatti essere l'articolo 6, paragrafo 1, lettera b) (contratto).

[25] Cfr. anche l'articolo 7, paragrafo 1, del regolamento generale sulla protezione dei dati, il quale stabilisce che il titolare del trattamento deve dimostrare che il consenso dell'interessato è stato liberamente manifestato.

[26] In una certa misura, l'introduzione di questo paragrafo è una codifica delle linee guida esistenti formulate dal Gruppo di lavoro Articolo 29. Come descritto nel parere 15/2011, quando un interessato si trova in una situazione di dipendenza rispetto al titolare del trattamento dei dati, in ragione della natura della relazione o di circostanze speciali, potrebbe sussistere una marcata presunzione che la libera manifestazione del consenso sia limitata in tali contesti (ad esempio in un rapporto di lavoro o se la raccolta dei dati è effettuata da un'autorità pubblica). Con l'entrata in vigore dell'articolo 7, paragrafo 4, sarà più difficile per il titolare del trattamento dimostrare che l'interessato ha prestato liberamente il consenso. Cfr.: parere 15/2011 del Gruppo di lavoro Articolo 29 sulla definizione di consenso (WP 187), pagg. 14-19.

[27] Come chiarito sopra, tali requisiti sono applicabili alle situazioni che rientrano nel campo di applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

[28] Ulteriori indicazioni sulla determinazione delle "finalità" sono riportate nel documento Opinion 3/2013 on purpose limitation [parere 3/2013 sulla limitazione della finalità] (WP 203).

[29] Il considerando 43 del regolamento generale sulla protezione dei dati afferma che, se del caso, sarà necessario un consenso separato per trattamenti distinti.
Dovrebbero essere messe a disposizione opzioni di consenso granulare in maniera da consentire agli interessati di acconsentire separatamente a finalità distinte.

[30] Cfr. il parere 3/2013 del Gruppo di lavoro Articolo 29 sulla limitazione della finalità (WP 203), pag. 16: *"Per questi motivi, una finalità che sia vaga o generica, come ad esempio 'migliorare l'esperienza degli utenti', 'finalità di marketing', 'finalità di sicurezza informatica' o 'ricerca futura', senza ulteriori dettagli, di solito non soddisfa i criteri per essere 'specifica'"*.

[31] Ciò è coerente con il parere 15/2011 del Gruppo di lavoro Articolo 29 sulla definizione di consenso (WP 187), ad esempio

a pag. 19.

[32] Cfr. anche il considerando 42 del regolamento generale sulla protezione dei dati: *"[…]Ai fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. […]"*.

[33] Ancora una volta, cfr. il considerando 42 del regolamento generale sulla protezione dei dati.

[34] Cfr. anche il parere 15/2011 del Gruppo di lavoro Articolo 29 sulla definizione di consenso (WP 187), pagg. 22-23.

[35] Cfr. l'articolo 7, paragrafo 3, del regolamento generale sulla protezione dei dati.

[36] Cfr. anche le linee guida del Gruppo di lavoro Articolo 29 sul processo decisionale automatizzato e la profilazione ai fini del regolamento 2016/679 (WP 251), punto IV.B, pag. 20 e successive.

[37] Ai sensi dell'articolo 49, paragrafo 1, lettera a), sono richieste informazioni specifiche sull'assenza delle garanzie di cui all'articolo 46, quando si richiede il consenso esplicito. Cfr. anche il parere 15/2011 del Gruppo di lavoro Articolo 29 sulla definizione di consenso (WP 187), pag. 20.

[38] La dichiarazione di consenso deve essere designata come tale. Scrivere formulazioni del tipo "So che..." non soddisfa il requisito di un linguaggio chiaro.

[39] Cfr. l'articolo 4, punto 11 e articolo 7, paragrafo 2, del regolamento generale sulla protezione dei dati.

[40] Cfr. anche il considerando 58 relativo a informazioni comprensibili per i minori.

[41] Cfr. anche il considerando 42 e la direttiva 93/13/CE, in particolare l'articolo 5 (linguaggio comprensibile e, in caso di dubbio, prevale l'interpretazione più favorevole al consumatore) e l'articolo 6 (invalidità di clausole abusive, il contratto continua a sussistere senza tali clausole abusive soltanto qualora sia ancora ragionevole, altrimenti l'intero contratto non è valido).

[42] Si noti che quando l'identità del titolare del trattamento o la finalità del trattamento non è evidente dal primo livello di informazioni dell'informativa sulla protezione dei dati a più livelli (e si trovano in ulteriori sottolivelli), sarà difficile per il titolare del trattamento dimostrare che l'interessato ha espresso il proprio consenso informato, a meno che il titolare del trattamento non possa dimostrare che l'interessato in questione ha avuto accesso a tali informazioni prima di manifestare il proprio consenso.

[43] Cfr. il documento di lavoro dei servizi della Commissione, Valutazione d'impatto, allegato 2, pag. 20 e anche pagg. 105-106 (in inglese): *"Come sottolineato anche nel parere adottato dal Gruppo di lavoro Articolo 29 in materia di consenso, sembra fondamentale chiarire che affinché un consenso sia valido è necessario ricorrere a meccanismi che non lascino dubbi circa l'intenzione dell'interessato di acconsentire, pur chiarendo che, nel contesto dell'ambiente online, l'uso di opzioni predefinite che l'interessato è tenuto a modificare per rifiutare il trattamento ('consenso basato sul silenzio') non costituisce di per sé un consenso inequivocabile. Ciò darebbe alle persone un controllo maggiore sui propri dati, qualora il trattamento si basi sul loro consenso. Per quanto riguarda l'impatto sui titolari del trattamento dei dati, ciò non avrebbe un impatto rilevante poiché chiarisce e specifica meglio le implicazioni della direttiva attuale in relazione alle condizioni per ottenere un consenso valido e significativo da parte dell'interessato. In particolare, nella misura in cui il consenso 'esplicito' chiarisca (sostituendo 'inequivocabile') le modalità e la qualità del consenso e che non è inteso a estendere i casi e le situazioni in cui il consenso (esplicito) verrebbe utilizzato come base giuridica per il trattamento, l'impatto di tale misura sui titolari del trattamento non dovrebbe essere rilevante"*.

[44] Cfr. l'articolo 7, paragrafo 2. Cfr. il documento di lavoro 2/2013 sull'ottenimento del consenso per i cookie (WP 208), pagg. 3-6.

[45] Cfr. il considerando 32 del regolamento generale sulla protezione dei dati.

[46] Il Gruppo di lavoro Articolo 29 ha sostenuto questa posizione in maniera coerente fin dal parere 15/2011 sulla definizione di consenso (WP 187), pagg. 35-37.

[47] Ai sensi dell'articolo 49, paragrafo 1, lettera a), del regolamento generale sulla protezione dei dati, il consenso esplicito può revocare il divieto di trasferimenti di dati verso paesi che non dispongono di livelli adeguati di protezione dei dati a norma di legge. Si consulti anche il documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE del 24 ottobre 1995 (WP 114), pag. 11, nell'ambito del quale il Gruppo di lavoro Articolo 29 ha indicato che il consenso per i trasferimenti di dati che si verificano periodicamente o su base continuativa è inappropriato.

[48] All'articolo 22 il regolamento generale sulla protezione dei dati introduce disposizioni destinate a proteggere gli interessati da un processo decisionale basato esclusivamente sul trattamento automatizzato, nonché dalla profilazione. Le decisioni adottate su tale base sono consentite nel rispetto di determinate condizioni legali. Il consenso svolge un ruolo chiave in questo meccanismo di protezione, in quanto l'articolo 22, paragrafo

2, lettera c), del regolamento generale sulla protezione dei dati, chiarisce che un titolare del trattamento può svolgere un processo decisionale automatizzato, compresa la profilazione, che può influire in maniera significativa sulle persone fisiche, con il consenso esplicito dell'interessato. Il Gruppo di lavoro Articolo 29 ha prodotto linee guida distinte su questo tema: Gruppo di lavoro Articolo 29, Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679 [Linee guida sul processo decisionale automatizzato e la profilazione ai fini del regolamento 2016/679], 3 ottobre 2017 (WP 251).

[49] Cfr. anche il parere 15/2011 del Gruppo di lavoro Articolo 29 sulla definizione di consenso (WP 187), pag. 29.

[50] Questo esempio non pregiudica il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

[51] Cfr. le linee guida del Gruppo di lavoro Articolo 29 sulla trasparenza ai sensi del regolamento 2016/679 WP260 rev.01 - approvate dal Comitato.

[52] Il Gruppo di lavoro Articolo 29 ha discusso questo argomento nel parere sul consenso (parere 15/2011 sulla definizione di consenso (WP 187), pagg. 11, 14, 23, 32 e 38-39) e, tra l'altro, nel parere sull'uso dei dati relativi all'ubicazione (parere 5/2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto (WP 115), pag. 7).

[53] Cfr. anche i seguenti pareri del Gruppo di lavoro Articolo 29: parere 4/2010 sul codice di condotta europeo della FEDMA per l'utilizzazione dei dati personali nel marketing diretto (WP 174) e parere 5/2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto (WP 115).

[54] Il considerando 39 del regolamento generale sulla protezione dei dati, che fa riferimento ai suoi articoli 13 e 14, afferma che *"[è] opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento"*.

[55] Cfr. l'articolo 17, paragrafo 1, lettera b) e l'articolo 17, paragrafo 3, del regolamento generale sulla protezione dei dati.

[56] In tal caso, l'altra finalità che giustifica il trattamento deve disporre di una propria base legittima distinta. Ciò non significa che il titolare del trattamento possa passare dal consenso a un'altra base legittima, cfr. la seguente sezione 6.

[57] Cfr. l'articolo 17, comprese le eccezioni che possono essere applicabili, e il considerando 65 del regolamento generale sulla protezione dei dati.

[58] Cfr. anche l'articolo 5, paragrafo 1, lettera e), del regolamento generale sulla protezione dei dati.

[59] Ai sensi dell'articolo 13, paragrafo 1, lettera c) e/o dell'articolo 14, paragrafo 1, lettera c), il titolare del trattamento è tenuto a informarne l'interessato.

[60] Fatta salva la possibilità per il diritto degli Stati membri di derogare al limite di età, cfr. l'articolo 8, paragrafo 1.

[61] Il considerando 58 del regolamento generale sulla protezione dei dati riafferma questo obbligo, dichiarando che, se del caso, il titolare del trattamento dovrebbe assicurarsi di fornire informazioni comprensibili per i minori.

[62] Ai sensi dell'articolo 4, paragrafo 25, del regolamento generale sulla protezione dei dati, per servizio della società dell'informazione si intende un servizio di cui all'articolo 1, paragrafo 1, lettera b), della direttiva 2015/1535: *"b) 'servizio': qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Ai fini della presente definizione si intende per: i) 'a distanza': un servizio fornito senza la presenza simultanea delle parti; ii) 'per via elettronica': un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici o altri mezzi elettromagnetici; iii) 'a richiesta individuale di un destinatario di servizi': un servizio fornito mediante trasmissione di dati su richiesta individuale"*. Nell'allegato I di detta direttiva figura un elenco indicativo di servizi non contemplati da tale definizione. Cfr. anche il considerando 18 della direttiva 2000/31/CE.

[63] Secondo la Convenzione delle Nazioni Unite sulla protezione dei minori, articolo 1, *"[...] si intende per fanciullo ogni essere umano avente un'età inferiore a diciott'anni, salvo se abbia raggiunto prima la maturità in virtù della legislazione applicabile"*, cfr. risoluzione 44/25 dell'Assemblea Generale delle Nazioni Unite del 20 novembre 1989 (Convenzione sui diritti del fanciullo).

[64] Cfr. la sentenza della Corte di giustizia, 2 dicembre 2010, nella causa C-108/09, (*Ker-Optika*), punti 22 e 28. In relazione ai "servizi compositi", il Comitato fa riferimento anche alla causa C-434/15 (*Asociacion Profesional Elite Taxi/Uber Systems Spain SL*), punto 40, al quale si afferma che un servizio della società dell'in-

formazione che costituisce parte integrante di un servizio generale la cui componente principale non è un servizio della società dell'informazione (in questo caso un servizio di trasporto), non rientra nella qualificazione di "servizio della società dell'informazione".

[65] Sebbene non sia una soluzione ideale in tutti i casi, è un esempio per rispondere a tale disposizione.

[66] Cfr. Opinion 5/2009 on social networking services [Parere 5/2009 Gruppo di lavoro Articolo 29 sui servizi di rete sociale] (WP 163) (in inglese).

[67] Il Comitato osserva che non sempre il titolare della responsabilità genitoriale è il genitore naturale del minore e che la responsabilità genitoriale può essere detenuta da più parti che possono comprendere tanto persone fisiche quanto persone giuridiche.

[68] Ad esempio a un genitore o un tutore potrebbe essere chiesto di effettuare un pagamento di 0,01 EUR al titolare del trattamento tramite una transazione bancaria, nonché una breve conferma nella riga descrittiva della transazione che il titolare del conto bancario è titolare della responsabilità genitoriale rispetto all'utente. Se del caso, dovrebbe essere previsto un metodo alternativo di verifica per evitare un indebito trattamento discriminatorio nei confronti delle persone che non dispongono di un conto bancario.

[69] Inoltre, gli interessati dovrebbero essere consapevoli del diritto all'oblio di cui all'articolo 17, che è particolarmente rilevante per il consenso dato quando l'interessato era ancora un minore, cfr. considerando 63.

[70] Cfr. anche il considerando 161 del regolamento generale sulla protezione dei dati.

[71] L'articolo 6, paragrafo 1, lettera c), può anche essere applicabile a parti dei trattamenti specificamente richiesti dalle disposizioni di legge, come la raccolta di dati affidabili e solidi secondo il protocollo approvato dallo Stato membro ai sensi del regolamento sulla sperimentazione clinica.

[72] La sperimentazione specifica di medicinali può aver luogo sulla base di una legislazione UE o nazionale ai sensi dell'articolo 9, paragrafo 2, lettera i).

[73] Cfr. ad esempio il considerando 156. Il trattamento di dati personali a fini scientifici dovrebbe inoltre essere conforme ad altre normative pertinenti come quella sulle sperimentazioni cliniche; cfr. il considerando 156 che menziona il regolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano. Cfr. anche il parere 15/2011 del Gruppo di lavoro Articolo 29 sulla definizione di consenso (WP 187), pag. 8: *"l'ottenimento del consenso non esonera il titolare del trattamento dagli obblighi di cui all'articolo 6 con riferimento ai principi di lealtà, necessità e proporzionalità, oltre che di qualità dei dati. Per esempio, anche qualora il trattamento dei dati personali poggi sul consenso dell'utilizzatore, ciò di per sé non legittima una raccolta dei dati supplementare rispetto allo scopo specifico.[...] In linea di principio, il consenso non dev'essere considerato come una forma di esonero dagli altri principi di protezione dei dati, bensì come una salvaguardia. Esso è, in prima linea, un motivo di liceità e non comporta una rinuncia all'applicazione di altri principi".*

[74] Possono essere pertinenti anche altre misure di trasparenza. Quando i titolari del trattamento svolgono un trattamento di dati a fini scientifici, nonostante non sia possibile fornire informazioni complete sin dall'inizio, possono comunque designare un referente specifico al quale gli interessati possono rivolgere eventuali quesiti.

[75] Tale possibilità si può riscontrare nell'articolo 14, paragrafo 1, dell'attuale legge sui dati personali della Finlandia (Henkilötietolaki, 523/1999).

[76] Cfr. anche il parere 5/2014 del Gruppo di lavoro Articolo 29 sulle tecniche di anonimizzazione (WP 216).

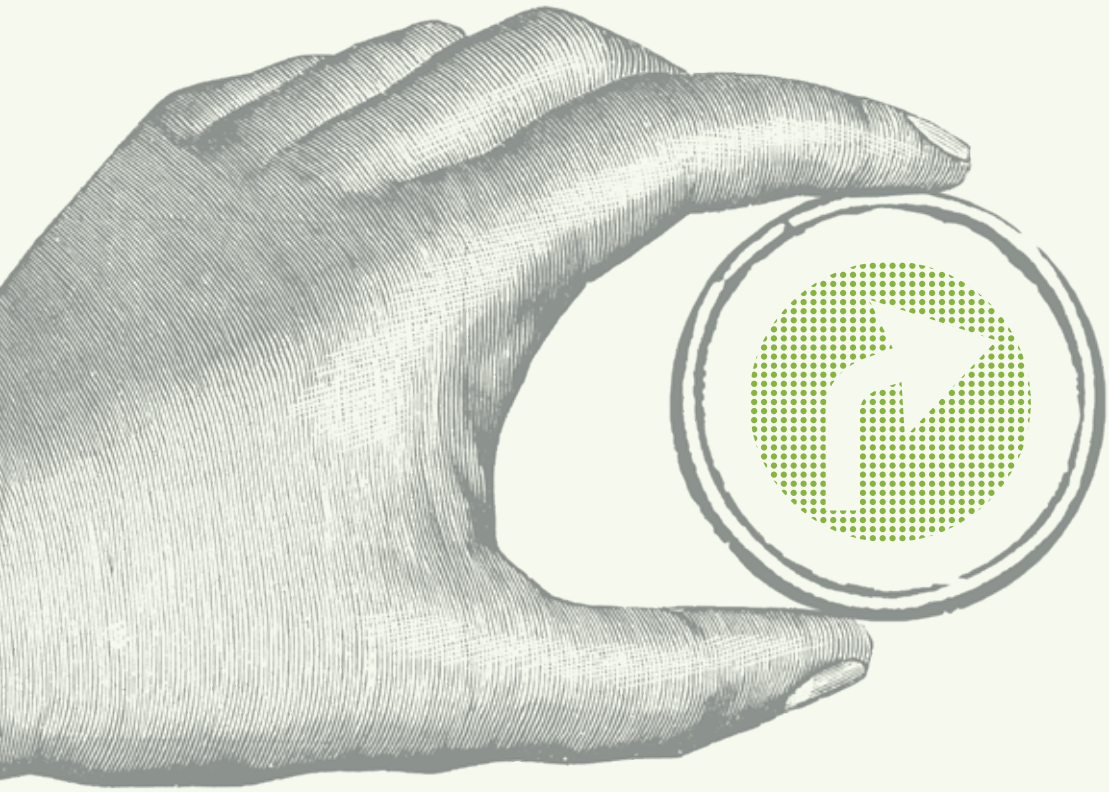
[77] Nei casi in cui determinate attività di trattamento dei dati sono limitate ai sensi dell'articolo 18, può essere necessario il consenso dell'interessato per annullare le limitazioni interessate.

[78] Il considerando 171 del regolamento generale sulla protezione dei dati afferma: *"Il presente regolamento dovrebbe abrogare la direttiva 95/46/CE. Il trattamento già in corso alla data di applicazione del presente regolamento dovrebbe essere reso conforme al presente regolamento entro un periodo di due anni dall'entrata in vigore del presente regolamento. Qualora il trattamento si basi sul consenso a norma della direttiva 95/46/CE, non occorre che l'interessato presti nuovamente il suo consenso, se questo è stato espresso secondo modalità conformi alle condizioni del presente regolamento, affinché il titolare del trattamento possa proseguire il trattamento in questione dopo la data di applicazione del presente regolamento. Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate".*

[79] Come indicato nell'introduzione, il regolamento generale sulla protezione dei dati fornisce ulteriori chiarimenti e specifiche sui requisiti per ottenere e dimostrare un consenso valido. Molti dei nuovi requisiti si basano sul parere 15/2011 sul consenso.

Torna a **Indice**

2 Obblighi di titolari e responsabili - accountability



Premessa
Obblighi di titolari e responsabili - accountability

Il principio detto di "accountability", ossia di responsabilizzazione, è probabilmente la novità più rilevante del GDPR per quanto riguarda l'approccio complessivo alla gestione dei dati personali. In estrema sintesi, esso consiste nell'obbligo per il titolare o il responsabile del trattamento di garantire il rispetto delle norme sulla protezione dei dati attraverso strumenti e atti idonei a dimostrare tale rispetto. Fondamentale al riguardo la considerazione dei rischi associati al trattamento dei dati personali, rischi che devono essere valutati e mitigati opportunamente.

Fra gli obblighi di sostanza che il GDPR ha esteso a tutti i titolari, e che precedentemente si applicavano solo ai fornitori di servizi di comunicazione elettronica accessibili al pubblico in base alla direttiva e-privacy (2002/58/CE), vi è anche quello di notificare al Garante (e di comunicare agli interessati, ove i rischi derivanti dalla violazione per i diritti e le libertà degli interessati siano particolarmente alti) le violazioni di dati personali (o "data breach"). Attraverso le **linee guida 1/2021**, l'EDPB ha fornito indicazioni ed esempi ulteriori rispetto alla notifica di violazioni di dati personali prendendo in esame alcune situazioni-tipo (attacchi con e senza esfiltrazione dei dati, in presenza o meno di backup, errori umani, ecc.) e descrivendo le misure di mitigazione del rischio più idonee alla luce delle misure già in essere nonché gli obblighi incombenti ai titolari nei singoli casi (notifica all'autorità, comunicazione agli interessati, tenuta di un registro delle violazioni).

Una delle chiavi di volta dell'approccio "basato sul rischio" che sottintende l'intero GDPR e lo stesso principio di responsabilizzazione è costituito dal principio cosiddetto di '*data protection by design and by default*' (DPbDD), ossia di protezione dei dati fin dalla progettazione e per impostazione predefinita. Attraverso le **linee guida 4/2019**, il Comitato ha voluto fornire indicazioni per l'attuazione efficace dei principi, dei diritti e delle libertà degli interessati in linea con tale principio, evidenziando, fra l'altro, come tutti i titolari, anche quelli di piccole dimensio-

ni, debbano adottare adeguate misure tecniche ed organizzative per soddisfare i requisiti del GDPR in materia di DPbDD. In questa prospettiva, le linee guida elencano elementi per attuare efficacemente i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita facendo ricorso ad esempi, anche rispetto all'utilizzo di meccanismi di certificazione. Significative le 11 raccomandazioni contenute nel documento che mirano a facilitare la cooperazione fra titolari e responsabili del trattamento nonché fornitori di tecnologia al fine di raggiungere gli obiettivi di DPbDD.

Non meno significativo è il contributo interpretativo fornito attraverso le **linee guida 7/2020 sui concetti di titolare e responsabile del trattamento**, che ha permesso di sistematizzare l'analisi di alcuni elementi essenziali di tali figure-cardine (in senso soggettivo e oggettivo) e, soprattutto, di chiarire gli ambiti del rapporto, di natura contrattuale, che deve intercorrere fra titolare e responsabile del trattamento ai sensi del GDPR con particolare riguardo ai requisiti di affidabilità del responsabile (di cui il titolare deve tenere conto ai fini della sua designazione) e agli elementi che devono figurare nel contratto o altro atto giuridico necessario a regolare i loro rapporti ai sensi del GDPR. Il testo si sofferma anche sulla nozione di contitolarità e fornisce alcuni criteri-guida al riguardo, quali l'oggettiva impossibilità di svolgere un trattamento senza la partecipazione dell'altro o degli altri titolari, ovvero l'inseparabilità del trattamento svolto da un titolare rispetto a quello effettuato dall'altro o dagli altri titolari. Occorre ricordare, in questo contesto, che la Commissione europea ha approvato (con il parere favorevole del Comitato) clausole contrattuali tipo per i contratti fra titolari e responsabili del trattamento (**Decisione di esecuzione 2021/915**), che costituiscono un importante contributo in termini di armonizzazione e certezza giuridica a livello Ue nonché di promozione di un approccio responsabilizzante.

Quale strumento atto a dimostrare il rispetto delle norme in materia di protezione dei dati, il GDPR ha introdotto la possibilità per i titolari di fare affidamento sulla certificazione di prodotti o servizi connessi al trattamento di dati personali, lasciando liberi i singoli Stati di decidere come organizzare il sistema nazionale di certificazione. Il meccanismo della certificazione prevede che quest'ultima sia rilasciata in ogni caso da soggetti "accreditati" da terze parti, e per questo il GDPR dedica due articoli (42, 43) alla definizione dei meccanismi di accreditamento, di nuovo lasciando agli Stati membri la possibilità di stabilire la ripartizione delle competenze in materia –se debba cioè essere un organismo nazionale di accreditamento a norma del Regolamento (Ue) 765/2008 o l'Autorità nazionale di controllo, oppure entrambi, a rilasciare l'accreditamento di organismi di certificazione in materia di protezione dei dati. In ogni caso le autorità di controllo sono tenute ad approvare requisiti specifici, orientati alle garanzie di protezione dei dati, che integrano quelli fissati nelle norme internazionali di riferimento e che devono essere applicati da tutti i soggetti competenti per l'accreditamento. Il Garante ha provveduto nel 2020 ad approvare i "**Requisiti aggiuntivi di accreditamento degli organismi di certificazione**" attenendosi strettamente alle indicazioni fornite dal Comitato nelle Linee guida 4/2018 in materia di accreditamento; si deve ricordare che, ai sensi del Codice 196/2003, l'accreditamento viene effettuato in Italia dall'ente nazionale di accreditamento, ossia ACCREDIA.

Un altro degli strumenti di natura volontaria utili per i titolari e responsabili del trattamento al fine di dimostrare la conformità al RGPD e per conquistare la fiducia degli interessati è rappresentato dai **codici di condotta**. Il Comitato è intervenuto in materia (**linee guida 1/2019**) fornendo chiarimenti interpretativi e orientamenti pratici in merito all'applicazione degli artt. 40 e 41 del RGPD. Tra gli obiettivi delle linee guida, quello di chiarire le procedure e le norme relative alla presentazione, all'approvazione e alla pubblicazione dei codici di condotta a livello sia nazionale che europeo, nonché quello di fornire un quadro di riferimento utile alle autorità di controllo, al Comitato e alla Commissione affinché la valutazione dei codici sia effettuata in modo coerente. Poiché, inoltre, i progetti di codice di condotta che contemplano attività di trattamento di enti non pubblici devono identificare un organismo di monitoraggio, esterno o interno, e descrivere i meccanismi attraverso i quali tale organismo potrà svolgere le sue funzioni di controllo sull'osservanza del codice da parte dei soggetti aderenti, le linee guida chiariscono quali criteri devono applicarsi alla costituzione e al funzionamento di tale organismo (requisiti di indipendenza rispetto agli aderenti al codice, assenza di conflitti di interesse, presenza di competenze adeguate), il quale potrà operare solo dopo essere stato accreditato dall'autorità di controllo competente ai sensi dell'art. 41, par. 1, del RGPD sulla base dei requisiti di accreditamento definiti dalla medesima autorità e approvati dal Comitato nell'ambito del meccanismo di coerenza di cui all'art. 63 del RGPD. Il Garante ha provveduto all'adozione di tali "**Requisiti di accreditamento degli organismi di monitoraggio dei codici di condotta**" nel corso del 2020.

Sempre nell'ottica di favorire la piena applicazione del principio di responsabilizzazione, il comitato si è impegnato a fornire indicazioni interpretative rispetto ad alcuni concetti e norme-chiave del GDPR in specifici contesti di particolare rilevanza o significatività.

È questo il caso delle **linee guida sul trattamento dei dati ai sensi dell'art. 6, par. 1, lett. b), del GDPR nell'ambito dei servizi online** (linee guida 2/2019), che esaminano l'interpretazione della norma del GDPR che prevede la liceità del trattamento ove esso sia necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso. Le linee guida, che si concentrano sui trattamenti effettuati online, sottolineano che l'art. 6(1), lettera b) del GDPR costituisce una valida base giuridica solo quando il trattamento è oggettivamente necessario all'esecuzione del contratto e che nella valutazione della necessità occorre tenere conto, in base al principio di correttezza del trattamento, anche delle "ragionevoli aspettative dell'interessato", considerato che spesso si tratta di contratti per adesione unilateralmente determinati dal fornitore del servizio online. Il documento esamina anche il caso dei trattamenti necessari al miglioramento del servizio, alla prevenzione delle frodi e alla pubblicità comportamentale (behavioural advertising) ed esclude, in linea generale, che tali trattamenti possano fondarsi sull'art. 6, par. 1, lett. b).

Anche alla luce delle novità tecnologiche che negli ultimi anni hanno caratterizzato l'ambito della videosorveglianza, il Comitato ha adottato nuove **linee**

guida sulla videosorveglianza (linee guida 3/2019) con l'obiettivo di garantire un'applicazione coerente dei principi del GDPR. Le linee guida riguardano sia i dispositivi video tradizionali sia i dispositivi video intelligenti analizzando, tra l'altro, la liceità del trattamento, l'applicabilità dei criteri di esclusione relativi ai trattamenti per finalità strettamente personali e la diffusione di filmati a terzi. Il Comitato considera che l'utilizzo della videosorveglianza, per le implicazioni in termini di diritti delle persone, sia da ammettere solamente quando gli scopi perseguiti non possono essere raggiunti con altre modalità meno invasive, e propone alcune soluzioni atte a minimizzare la raccolta dei dati (per esempio cancellazione automatica mediante sovrascrittura del registrato, con video accessibili solo in caso di necessità). Viene inoltre ribadita la necessità di una valutazione di impatto ogniqualvolta vi sia una sorveglianza sistematica su larga scala di una zona accessibile al pubblico, e della designazione di un RPD nei casi in cui vi sia un monitoraggio regolare e sistematico degli interessati su larga scala.

Con le **linee guida 01/2020 sul trattamento di dati personali nell'ambito dell'uso dei veicoli connessi e delle applicazioni relative alla mobilità**, il Comitato ha fornito indicazioni sui trattamenti di dati personali all'interno del veicolo e scambiati tra il veicolo e i dispositivi personali ad esso collegati (ad es. lo smartphone dell'utente) o raccolti all'interno del veicolo e trasmessi ad entità esterne per ulteriori elaborazioni (ad es. costruttori di veicoli, gestori di infrastrutture, compagnie di assicurazione, autoriparatori). Il documento evidenzia i rischi connessi a tali tipologie di trattamento e le misure da adottare per assicurare il rispetto della disciplina in materia di protezione dei dati personali. La regolamentazione dei veicoli connessi vede infatti il coinvolgimento di una pluralità di attori appartenenti sia al settore automobilistico sia a quello digitale, ciascuno dei quali riveste generalmente il ruolo soggettivo di titolare autonomo del trattamento o di contitolare ed anche, in taluni casi, quello di responsabile del trattamento.

Le importanti novità nel sistema dei pagamenti introdotte dalla direttiva (UE) 2015/2366 sui servizi di pagamento (PSD2) – che consente a nuovi soggetti di attuare servizi che un tempo erano prerogativa esclusiva delle banche, e quindi di accedere a una mole considerevole di dati finanziari anche di soggetti terzi – ha reso necessaria una riflessione sul corretto rapporto tra la PSD2 e il GDPR attraverso le **linee guida 06/2020**. I temi affrontati riguardano, in particolare, le basi giuridiche del trattamento effettuato dai fornitori di servizi di pagamento, i cosiddetti "ulteriori trattamenti" alla luce della PSD2 (che in ogni caso già prevede un approccio restrittivo in materia, limitando considerevolmente la possibilità di trattamenti per finalità ulteriori rispetto a quelle originariamente previste), il trattamento dei dati sensibili anche con riferimento alle *silent third parties* (ad es. i beneficiari di ordini di pagamenti), e l'applicazione dei principi di minimizzazione dei dati, sicurezza, trasparenza e accountability.

Le **linee guida sul *targeting* degli utenti di social media (08/2020)** rappresentano un importante documento in considerazione dello sviluppo significativo registrato dalle reti sociali online nell'ultimo decennio. Numerosi fornitori di social media offrono servizi di *targeting* che consentono a persone fisiche o giu-

ridiche (*targeter*) di comunicare messaggi specifici agli utenti per promuovere interessi commerciali, politici o di altro tipo, nonché funzioni aggiuntive quali la personalizzazione, l'integrazione di applicazioni, i plug-in sociali. In tale contesto, le linee guida forniscono chiarimenti per quanto riguarda la contitolarità del trattamento effettuato in questi casi (fra il soggetto che intende promuovere prodotti o servizi e il social network che offre strumenti per campagne promozionali mirate), in virtù del legame inestricabile che si crea fra i due operatori di trattamento. Il Comitato evidenzia, inoltre, che la base giuridica dei trattamenti in questione non può consistere nell'adempimento di obblighi contrattuali (art. 6, par. 1, lett. b), del GDPR) da parte della piattaforma di social media né da parte dei *targeter* poiché, in particolare, il *targeting* degli utenti non rappresenta un elemento intrinsecamente necessario del rapporto contrattuale con l'interessato.

Le **linee guida sugli assistenti vocali virtuali (AVV) 2/2021** esaminano i servizi che comprendono i comandi vocali e li eseguono ovvero, se necessario, mediano con altri sistemi informatici; si tratta di servizi disponibili sulla maggior parte degli smartphone e dei tablet, sui computer tradizionali e, negli ultimi anni, anche su dispositivi stand-alone come gli altoparlanti intelligenti, e che pertanto hanno accesso a un'enorme quantità di dati personali fra cui tutti i comandi impartiti dagli utenti ai loro dispositivi (come la cronologia di navigazione o di ricerca) e le risposte degli stessi (appuntamenti in agenda). Le linee guida confermano la necessità di implementare adeguate misure di sicurezza e di garanzia, di applicare i principi di privacy by design e di privacy by default e di ricorrere agli strumenti di accountability previsti espressamente dal Regolamento. Inoltre, il provider dei servizi AVV deve fornire agli interessati tutte le informazioni previste dal GDPR, in una forma semplice, chiara e accessibile, compresi gli utenti accidentali – pur riconoscendo che, nella pratica, tale condizione è difficile da rispettare allo stato attuale delle conoscenze.

Con le **raccomandazioni 02/2021 sulla conservazione dei dati relativi a carte di credito da parte di piattaforme online**, il Comitato ha voluto indicare alcune buone prassi per i titolari (le piattaforme online) rispetto a tutte quelle situazioni in cui gli interessati acquistano un prodotto o pagano un servizio tramite un sito web o un'applicazione con carta di credito, il cui numero viene memorizzato per evitare che il cliente debba nuovamente digitarlo nei successivi acquisti. Si segnala, in proposito, come l'unica base giuridica appropriata di cui il titolare può servirsi per conservare i dati della carta di credito dopo l'acquisto sia il consenso specifico, fornito mediante un'azione positiva inequivocabile; il consenso al trattamento deve essere distinto da quello fornito per le condizioni di servizio o di vendita, non può costituire una condizione per la realizzazione dell'operazione, e deve inoltre essere revocabile in qualsiasi momento, con la stessa facilità con cui è stato fornito.

Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679 Versione 2.0

4 giugno 2019

Cronologia delle versioni

Versione 2.0	4 giugno 2019	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	12 febbraio 2019	Adozione delle linee guida per la consultazione pubblica

Indice

1 Introduzione
1.1 Campo d'applicazione delle linee guida

2 Definizioni

3 Che cosa sono i codici?

4 Quali benefici apportano i codici?

5 Ammissibilità di un progetto di codice
5.1 Motivazione e documenti giustificativi
5.2 Rappresentante
5.3 Ambito di trattamento
5.4 Ambito di applicazione territoriale
5.5 Presentazione a un'autorità di controllo competente
5.6 Meccanismi di vigilanza
5.7 Organismo di monitoraggio
5.8 Consultazione
5.9 Normativa nazionale
5.10 Lingua
5.11 Lista di controllo

6 Criteri di approvazione dei codici
6.1 Soddisfa una particolare esigenza
6.2 Facilita l'efficace applicazione del regolamento
6.3 Precisa l'applicazione del regolamento
6.4 Offre sufficienti garanzie
6.5 Offre meccanismi che consentiranno un controllo efficace

7 Presentazione, ammissibilità e approvazione (codice nazionale)
7.1 Presentazione
7.2 Ammissibilità di un codice
7.3 Approvazione

8 Presentazione, ammissibilità e approvazione (codice transnazionale)
8.1 Presentazione
8.2 Ammissibilità di un codice
8.3 Cooperazione
8.4 Rigetto
8.5 Preparazione ai fini della presentazione al comitato

8.6 Il comitato
8.7 Approvazione

9 Coinvolgimento

10 Il ruolo della commissione

11 Monitoraggio di un codice

12 Requisiti di accreditamento per gli organismi di monitoraggio
12.1 Indipendenza
12.2 Conflitto di interessi
12.3 Competenze
12.4 Procedure e strutture consolidate
12.5 Gestione trasparente dei reclami
12.6 Comunicazione con l'autorità di controllo competente
12.7 Meccanismi di riesame
12.8 Status giuridico

13 Codici approvati

14 Revoca di un organismo di monitoraggio

15 Codici del settore pubblico

Appendice 1 - distinzione tra codici nazionali e transnazionali
Appendice 2 - scegliere l'autorità di controllo competente
Appendice 3 - lista di controllo per la presentazione
Appendice 4 - diagramma di flusso per un codice transnazionale

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettera n), e gli articoli 40 e 41 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati),

visto l'accordo sullo Spazio economico europeo (SEE), in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del comitato misto SEE n. 154/2018 del 6 luglio 2018,

visto l'articolo 12 e l'articolo 22 del regolamento interno del 25 maggio 2018,

HA ADOTTATO IL SEGUENTE PARERE:

1. INTRODUZIONE

1. Il regolamento (UE) 2016/679[1] ("regolamento") è entrato in applicazione il 25 maggio 2018. Uno dei suoi obiettivi principali è assicurare un livello coerente di protezione dei dati in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno[2]. Il regolamento introduce anche il principio di responsabilizzazione, che impone al titolare del trattamento la responsabilità di conformarsi al regolamento e di dimostrare la conformità[3]. Le disposizioni di cui agli articoli 40 e 41 del regolamento riguardo ai codici di condotta ("codici") rappresentano un metodo pratico, potenzialmente economico e significativo per ottenere maggiori livelli di coerenza nella tutela dei diritti in materia di protezione dei dati. I codici possono fungere da meccanismo attraverso il quale dimostrare la conformità al regolamento[4]. In particolare, essi possono contribuire a colmare gli eventuali divari di armonizzazione esistenti tra gli Stati membri nell'applicazione della normativa in materia di protezione dei dati[5]. Offrono inoltre l'opportunità a determinati settori di riflettere su attività comuni di trattamento dei dati e di concordare regole pratiche e su misura per la protezione dei dati, che soddisfino le esigenze del settore e i requisiti del regolamento[6].
2. Gli Stati membri, le autorità di controllo, il comitato europeo per la protezione dei dati ("comitato") e la Commissione europea ("Commissione") sono tenuti a incoraggiare l'elaborazione di codici destinati a contribuire alla corretta applicazione del regolamento[7]. Le presenti linee guida sosterranno e agevoleranno i "titolari dei codici" nell'elaborazione, nella modifica e nella proroga dei codici.

1.1 CAMPO D'APPLICAZIONE DELLE LINEE GUIDA

3. Lo scopo delle presenti linee guida è offrire orientamenti pratici e assistenza interpretativa in relazione all'applicazione degli articoli 40 e 41 del regolamento. Esse sono intese a chiarire le procedure e le regole per la presentazione, l'approvazione e la pubblicazione dei codici, a livello sia nazionale che europeo. Intendono inoltre definire i criteri minimi richiesti da un'autorità di controllo competente per poter effettuare un esame e una valutazione approfonditi di un codice[8]. Intendono altresì stabilire i fattori di contenuto da prendere in considerazione nel valutare se un determinato codice contribuisca alla corretta ed efficace applicazione[9] del regolamento. Infine, le linee guida sono intese a stabilire i requisiti per il controllo efficace della conformità con un codice[10].
4. Le presenti linee guida mirano inoltre a offrire a tutte le autorità di controllo competenti, al comitato e alla Commissione un quadro di riferimento chiaro che permetta di valutare i codici in modo coerente e di semplificare le procedure previste dal processo di valutazione. Tale quadro dovrebbe inoltre offrire maggiore trasparenza e consentire ai titolari dei codici che intendono chiedere l'approvazione di un codice di avere piena familiarità con il proces-

so e comprendere i requisiti formali e i criteri di adeguatezza richiesti per l'approvazione.

5. Orientamenti sui codici di condotta come strumento per i trasferimenti di dati, conformemente all'articolo 40, paragrafo 3, del regolamento, saranno oggetto di distinte linee guida emanate dal comitato.
6. Tutti i codici precedentemente approvati[11] dovranno essere riesaminati e nuovamente valutati in linea con i requisiti del regolamento, per essere successivamente ripresentati per approvazione conformemente al disposto degli articoli 40 e 41 e alle procedure descritte nel presente documento.

2. DEFINIZIONI

"Accreditamento": l'accertamento volto a verificare che l'organismo di monitoraggio proposto soddisfi i requisiti di cui all'articolo 41 del regolamento ai fini del controllo della conformità con un codice di condotta. Questa verifica viene effettuata dall'autorità di controllo cui viene presentato il codice per approvazione (articolo 41, paragrafo 1). L'accreditamento di un organismo di monitoraggio vale soltanto per un codice specifico[12].

"Titolari dei codici": associazioni o altre organizzazioni che elaborano e presentano un codice[13] che avranno uno status giuridico adeguato, conformemente al codice e alla legislazione nazionale.

"Autorità di controllo competente": l'autorità di controllo competente ai sensi dell'articolo 55 del regolamento.

"Organismo di monitoraggio": un organismo/comitato o diversi organismi/comitati (interni o esterni ai titolari dei codici[14]) che svolgono una funzione di monitoraggio al fine di accertare e assicurare il rispetto del codice ai sensi dall'articolo 41.

"Autorità di controllo interessate": le autorità di cui all'articolo 4, punto 22, del regolamento.

"Codice nazionale": un codice che regola le attività di trattamento in uno Stato membro.

"Codice transnazionale": un codice che regola le attività di trattamento in più Stati membri.

3. CHE COSA SONO I CODICI?

7. I codici previsti dal regolamento sono strumenti di responsabilizzazione volontari che stabiliscono specifiche norme di protezione dei dati per categorie di titolari e di responsabili del trattamento. Essi possono essere un utile ed efficace strumento di responsabilizzazione in quanto forniscono una descrizione dettagliata dei comportamenti più appropriati, in termini giuridici ed etici, con riguardo a un determinato settore. Dal punto di vista della prote-

zione dei dati, i codici possono quindi fungere da decalogo per i titolari e i responsabili del trattamento che progettano e svolgono attività di trattamento dei dati conformi al regolamento, conferendo un significato operativo ai principi di protezione dei dati stabiliti dalla legislazione europea e nazionale.

8. Le associazioni o le organizzazioni rappresentative di un settore possono creare codici per aiutare il rispettivo settore a conformarsi al regolamento in modo efficiente e potenzialmente economico. Come indicato nell'elenco non esaustivo che figura all'articolo 40, paragrafo 2, del regolamento, i codici di condotta possono riguardare ambiti quali:

- il trattamento corretto e trasparente dei dati;
- i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;
- la raccolta dei dati personali; la pseudonimizzazione dei dati personali;
- l'informazione fornita alle persone e l'esercizio dei diritti delle persone;
- l'informazione fornita ai minori e la loro tutela (incluse le modalità con cui è ottenuto il consenso genitoriale);
- le misure tecniche e organizzative, inclusa la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita nonché le misure di sicurezza;
- la notifica di una violazione;
- il trasferimento di dati personali verso paesi terzi;
- le procedure di composizione delle controversie.

9. Il regolamento, abrogando la direttiva sulla protezione dei dati (95/46/CE), prevede disposizioni più specifiche e dettagliate sui codici, definisce i requisiti da soddisfare e le procedure da seguire per ottenerne l'approvazione e, una volta approvati, per la loro registrazione, pubblicazione e promozione. Tali disposizioni, unitamente alle presenti linee guida, serviranno a incoraggiare i titolari dei codici a contribuire direttamente alla definizione di standard e norme in materia di protezione dei dati per i rispettivi settori di trattamento.

10. È importante notare che i codici sono uno dei molti strumenti di natura volontaria utilizzabili nel quadro degli ausili di responsabilizzazione in materia di protezione dei dati offerti dal regolamento, quali le valutazioni d'impatto sulla protezione dei dati[15] e la certificazione[16]. Si tratta di un meccanismo che permette di aiutare titolari e responsabili del trattamento a dimostrare la loro conformità al regolamento[17].

4. QUALI BENEFICI APPORTANO I CODICI?

11. I codici rappresentano un'opportunità per stabilire una serie di regole che contribuiscano alla corretta applicazione del regolamento in modo pratico, trasparente e potenzialmente economico, tenendo conto delle specificità di

un particolare settore e/o dei trattamenti svolti in tale settore. A tale riguardo, i codici possono essere elaborati per i titolari e i responsabili del trattamento tenendo conto delle caratteristiche specifiche del trattamento effettuato in determinati settori e delle esigenze specifiche delle microimprese e delle piccole e medie imprese[18]. I codici sono uno strumento potenzialmente molto importante e vantaggioso per le PMI e le microimprese[19] perché permettono loro di rispettare le norme sulla protezione dei dati in modo più economico.

> Ad esempio, le microimprese che svolgono attività simili di ricerca sanitaria potrebbero coalizzarsi tramite le loro associazioni e sviluppare collettivamente un codice che disciplini la raccolta e il trattamento dei dati sanitari, anziché cercare di condurre da sole un'analisi approfondita della protezione dei dati. I codici andranno inoltre a beneficio delle autorità di controllo perché consentiranno loro di comprendere meglio le attività di trattamento di una specifica professione, di un'attività o settore.

12. I codici possono aiutare i titolari e i responsabili del trattamento a conformarsi al regolamento, disciplinando temi quali: il trattamento corretto e trasparente dei dati, i legittimi interessi, le misure di sicurezza e di protezione dei dati fin dalla progettazione e per impostazione predefinita, gli obblighi del titolare del trattamento. I codici sono accessibili a tutti i settori di trattamento e possono essere redatti in modo più specifico o più ampio a seconda del particolare settore[20], purché contribuiscano alla corretta ed efficace applicazione del regolamento[21].

> Ad esempio, si potrebbe chiedere l'approvazione di una serie di regole tese a garantire correttezza e trasparenza dei trattamenti svolti in un ambito specifico del terzo settore. In alternativa, si potrebbe decidere di redigere un codice, che incorpori e applichi correttamente una moltitudine di disposizioni del regolamento per coprire tutte le attività di trattamento in un ambito specifico del terzo settore, dall'individuazione del fondamento giuridico per la raccolta dei dati personali alla notifica delle violazioni dei dati personali.

13. I codici permettono un certo grado di co-regolazione e consentono ai titolari e ai responsabili del trattamento di non dipendere eccessivamente dalle autorità di controllo per disporre di orientamenti più granulari sulle specifiche attività di trattamento.
14. I codici possono offrire ai titolari e ai responsabili del trattamento un certo grado di autonomia e controllo nel formulare e concordare le buone prassi per gli specifici settori. Possono consentire di consolidare le migliori prassi riguardanti le operazioni di trattamento in specifici settori, e possono anche diventare una risorsa fondamentale per le imprese al fine di gestire aspetti

critici nelle procedure di trattamento e conseguire una migliore osservanza delle norme in materia di protezione dei dati.

15. I codici possono generare fiducia e certezza del diritto, elementi assolutamente necessari, offrendo soluzioni pratiche ai problemi identificati in particolari settori con riguardo ad attività di trattamento comuni. Essi favoriscono lo sviluppo di un approccio collettivo e coerente alle esigenze di trattamento dei dati di un particolare settore.

16. I codici possono essere uno strumento efficace per conquistare la fiducia degli interessati. Possono affrontare le più diverse questioni, molte delle quali derivano talora da preoccupazioni del pubblico o hanno origine all'interno del settore stesso, e, in quanto tali, costituiscono uno strumento per migliorare la trasparenza nei confronti delle persone riguardo al trattamento dei loro dati personali.

Ad esempio, nel contesto del trattamento dei dati sanitari a fini di ricerca, l'esistenza di un codice approvato contenente regole dettagliate potrebbe mitigare i timori sulle misure da adottare per promuovere il rispetto delle norme applicabili al trattamento di dati sanitari particolarmente sensibili. Tale codice potrebbe descrivere in maniera corretta e trasparente quanto segue:

- le garanzie pertinenti da applicare riguardo all'informazione agli interessati;
- le garanzie pertinenti da applicare riguardo ai dati raccolti presso terzi;
- la comunicazione o la diffusione dei dati;
- i criteri da attuare per garantire il rispetto del principio di minimizzazione dei dati;
- le specifiche misure di sicurezza;
- adeguati termini di conservazione;
- i meccanismi di gestione dei dati in seguito all'esercizio dei diritti degli interessati (conformemente agli articoli 32 e 89 del regolamento).

17. I codici possono costituire un meccanismo significativo e utile anche nel settore dei trasferimenti internazionali. Alcune nuove disposizioni del regolamento consentono a terzi di aderire ai codici approvati per soddisfare l'obbligo giuridico di fornire garanzie adeguate in relazione ai trasferimenti internazionali di dati personali verso paesi terzi[22]. Inoltre, i codici approvati di questo tipo possono promuovere e migliorare il livello di protezione che il regolamento offre alla più ampia comunità internazionale e permettere trasferimenti internazionali di dati personali sostenibili e conformi alla legge. I codici possono anche servire a sviluppare e a promuovere ulteriormente la fiducia degli interessati nel trattamento dei dati al di fuori dello Spazio economico europeo[23].

18. I codici approvati costituiscono potenzialmente efficaci strumenti di re-

sponsabilizzazione per i titolari e per i responsabili del trattamento. Come indicato nel considerando 77 e all'articolo 24, paragrafo 3, del regolamento, l'adesione a un codice di condotta approvato è considerata uno degli strumenti idonei a dimostrare la conformità a determinati settori o principi del regolamento o al regolamento nel suo complesso da parte di un titolare o di un responsabile del trattamento[24]. Inoltre, l'adesione a un codice di condotta approvato sarà un fattore preso in considerazione dalle autorità di controllo nel valutare caratteristiche specifiche di un trattamento, come gli aspetti relativi alla sicurezza[25], o nel valutare l'impatto del trattamento nell'ambito di una valutazione d'impatto sulla protezione dei dati[26] oppure nell'infliggere una sanzione amministrativa[27]. In caso di violazione di una delle disposizioni del regolamento, l'adesione a un codice di condotta approvato potrebbe segnalare la maggiore o minore necessità di intervenire con una sanzione amministrativa pecuniaria effettiva, proporzionata e dissuasiva ovvero ricorrere a un'altra misura correttiva dell'autorità di controllo[28].

5. AMMISSIBILITÀ DI UN PROGETTO DI CODICE[29]

19. Prima che un'autorità di controllo competente possa impegnarsi a valutare e a esaminare nei dettagli un codice di condotta ai fini dell'articolo 40, paragrafo 5, del regolamento, è necessario che siano soddisfatte alcune condizioni così da facilitare una valutazione efficiente. Si applicano i criteri seguenti.

5.1 MOTIVAZIONE E DOCUMENTI GIUSTIFICATIVI

20. Ogni progetto di codice presentato per approvazione deve contenere una motivazione chiara e concisa in cui siano specificati lo scopo del codice, l'oggetto[30] e in che modo esso faciliterà l'efficace applicazione del regolamento[31]. Ciò contribuirà ad accelerare il processo e ad assicurare la chiarezza richiesta per la presentazione del progetto di codice. All'atto della presentazione occorre includere la pertinente documentazione di supporto del progetto di codice e della motivazione[32].

5.2 RAPPRESENTANTE

21. Il codice deve essere presentato da un'associazione/un consorzio di associazioni o da altri enti che rappresentano categorie di titolari o di responsabili del trattamento (i "titolari" del codice) a norma dell'articolo 40, paragrafo 2. A titolo esemplificativo potrebbe trattarsi di associazioni di categoria e di rappresentanza, organizzazioni di settore, organizzazioni accademiche e gruppi di interesse.
22. I titolari del codice devono dimostrare all'autorità di controllo competente di

essere organismi rappresentativi efficaci, di saper comprendere le esigenze dei propri membri e di saper definire chiaramente l'attività o il settore di trattamento cui si applicherà il codice. In base alla definizione e ai parametri del settore interessato, la rappresentatività può essere ricavata, fra l'altro, dai seguenti elementi:

- numero o percentuale di potenziali aderenti al codice fra i titolari o i responsabili del trattamento operanti in tale settore;
- esperienza dell'organismo rappresentativo maturata nel settore e nelle attività di trattamento inerenti al codice.

5.3 AMBITO DI TRATTAMENTO

23. Il progetto di codice deve avere un ambito definito, che illustri in modo chiaro e preciso le operazioni di trattamento contemplate (o le caratteristiche del trattamento), nonché le categorie di titolari o di responsabili del trattamento interessate. La descrizione deve includere le problematiche di trattamento che il codice intende affrontare e le soluzioni pratiche proposte.

5.4 AMBITO DI APPLICAZIONE TERRITORIALE

24. Il progetto di codice deve indicare se si tratta di un codice nazionale o transnazionale e specificare l'ambito di applicazione territoriale, identificando tutte le giurisdizioni pertinenti in cui esso troverà applicazione. Per i codici transnazionali (e i codici transnazionali modificati o prorogati) va incluso un elenco delle autorità di controllo interessate. L'appendice 1 illustra le differenze tra i codici nazionali e quelli transnazionali.

5.5 PRESENTAZIONE A UN'AUTORITÀ DI CONTROLLO COMPETENTE

25. I titolari del codice devono assicurarsi che l'autorità di controllo individuata al fine di esaminare il progetto di codice sia competente a norma dell'articolo 55 del regolamento[33]. L'appendice 2 offre ulteriori informazioni di ausilio per i titolari del codice nell'individuazione dell'autorità di controllo competente per un codice transnazionale.

5.6 MECCANISMI DI VIGILANZA

26. Il progetto di codice deve proporre meccanismi attraverso i quali sia possibile vigilare sull'osservanza delle relative disposizioni da parte di chi si è impegnato ad applicarlo[34]. Ciò vale sia per i codici del settore pubblico che per i codici del settore non pubblico.

5.7 ORGANISMO DI MONITORAGGIO

27. Un progetto di codice che contempli attività di trattamento di autorità o enti privati, non pubblici, deve inoltre identificare un organismo di monitoraggio e descrivere i meccanismi attraverso i quali tale organismo può svolgere le sue funzioni ai sensi dell'articolo 41 del regolamento[35]. L'organismo o gli organismi di monitoraggio identificati devono avere uno status adeguato per soddisfare il requisito di piena responsabilità necessario per il loro ruolo[36]. A tal fine, l'organismo o gli organismi di monitoraggio devono essere accreditati dall'autorità di controllo competente ai sensi dell'articolo 41, paragrafo 1, del regolamento[37].

5.8 CONSULTAZIONE

28. Il progetto di codice deve contenere informazioni dettagliate sulle consultazioni effettuate. Il considerando 99 del regolamento indica che, nell'elaborare un codice (o nel modificare o prorogare tale codice), si dovrebbero consultare le parti interessate pertinenti, compresi, quando possibile, gli interessati. Pertanto, i titolari del codice dovrebbero confermare e dimostrare, al momento di presentare il codice per l'approvazione, che si sono svolte consultazioni adeguate con le parti interessate. Se del caso, dovranno includere informazioni su altri codici di condotta cui siano eventualmente soggetti gli aderenti potenziali del codice in esame e illustrare in che modo quest'ultimo vada a integrare altri codici. Dovrebbero inoltre descrivere il livello e la natura delle consultazioni tenute con i membri, con altre parti interessate e con gli interessati, o con le associazioni/organizzazioni che li rappresentano[38]. In pratica, si raccomanda vivamente di consultare i membri dell'organizzazione o dell'organismo che agisce in qualità di titolare del codice e, tenendo conto dell'attività di trattamento, anche i clienti di tali membri. Qualora non sia stato possibile consultare determinate parti interessate, sarà compito dei titolari del codice spiegare la situazione.

5.9 NORMATIVA NAZIONALE

29. I titolari del codice devono confermare che il progetto di codice è conforme alla pertinente normativa nazionale, in particolare se il codice riguarda un settore regolato da disposizioni specifiche del diritto nazionale o riguarda operazioni di trattamento che devono essere valutate sulla base di requisiti specifici e dei pertinenti obblighi giuridici ai sensi del diritto nazionale.

5.10 LINGUA

30. I titolari del codice devono osservare i requisiti linguistici dell'autorità di

controllo competente cui presenteranno il codice. In generale, il codice deve essere presentato nella lingua dell'autorità di controllo competente di quello Stato membro[39]. Per i codici transnazionali il codice deve essere presentato nella lingua dell'autorità di controllo competente e anche in inglese[40].

5.11 LISTA DI CONTROLLO

31. In ultima analisi sarà compito dell'autorità di controllo competente prescelta stabilire se il progetto di codice possa passare alla successiva fase di valutazione, ossia se l'autorità di controllo competente si impegni a effettuare una valutazione completa del contenuto in linea con gli articoli 40 e 41 del regolamento e le procedure indicate di seguito. La lista di controllo dell'appendice 3 serve a verificare la documentazione presentata a un'autorità di controllo competente e a inquadrare la presentazione del progetto di codice.

6. CRITERI DI APPROVAZIONE DEI CODICI

32. I titolari dei codici devono essere in grado di dimostrare in che modo il loro codice contribuirà alla corretta applicazione del regolamento, tenendo conto delle specificità dei vari settori di trattamento nonché dei requisiti e degli obblighi specifici dei titolari o dei responsabili del trattamento cui il codice si riferisce. Questo requisito generale comprende più aspetti. I titolari dei codici devono essere in grado di dimostrare che il loro progetto di codice:

- soddisfa una particolare esigenza di quel settore o di quella attività di trattamento,
- facilita l'applicazione del regolamento,
- precisa l'applicazione del regolamento,
- offre sufficienti garanzie[41] e
- offre meccanismi efficaci per controllare il rispetto del codice.

6.1 SODDISFA UNA PARTICOLARE ESIGENZA

33. I titolari dei codici devono dimostrare la necessità di creare un codice. Pertanto, un codice di condotta deve affrontare questioni riguardanti la protezione dei dati che emergono per un particolare settore o una particolare attività di trattamento.

> Ad esempio, il settore dei sistemi informativi per l'individuazione dei rischi del credito al consumo potrebbe avere la necessità di elaborare un codice per fornire garanzie e meccanismi sufficienti tali da assicurare che i dati raccolti siano pertinenti, esatti e utilizzati esclusivamente per

lo scopo specifico e legittimo di tutelare il credito. In modo analogo, il settore della ricerca sanitaria potrebbe individuare la necessità di formulare un codice che promuova un approccio coerente definendo norme volte a soddisfare adeguatamente l'obbligo del consenso esplicito e i connessi obblighi di responsabilizzazione previsti dal regolamento.

34. I titolari dei codici devono essere in grado di illustrare ordinatamente i problemi che il codice intende affrontare e di motivare in che modo le soluzioni offerte dal codice saranno efficaci e utili, non solo per gli aderenti, ma anche per gli interessati.

6.2 FACILITA L'EFFICACE APPLICAZIONE DEL REGOLAMENTO

35. Secondo il considerando 98 del regolamento, affinché il codice sia approvato, il titolare del codice deve essere in grado di dimostrare che esso facilita l'efficace applicazione del regolamento. A tale riguardo, il codice dovrà indicare chiaramente il carattere settoriale delle disposizioni di applicazione del regolamento in esso contenute nonché identificare ed esaminare le esigenze specifiche del settore[42].

Per facilitare l'efficace applicazione del regolamento è ad esempio possibile fornire un elenco di definizioni specifiche del settore e riservare un'attenzione adeguata alle tematiche particolarmente pertinenti per quel settore. L'uso di una terminologia settoriale per descrivere l'attuazione dei requisiti del regolamento in un dato settore può anche migliorare la comprensione delle regole nel settore e quindi facilitare l'efficace applicazione del regolamento. Un codice dovrebbe tenere pienamente conto dei probabili rischi connessi all'attività di trattamento di un particolare settore e calibrare opportunamente i relativi obblighi dei titolari o dei responsabili del trattamento cui tale codice si applica alla luce dei rischi suddetti propri di quel settore specifico, per esempio fornendo esempi di clausole accettabili in relazione all'uso di dati personali nel marketing diretto. In termini di formato, il contenuto del codice dovrebbe essere presentato in modo da agevolarne la comprensione e l'utilizzo e da facilitare l'efficace applicazione del regolamento.

6.3 PRECISA L'APPLICAZIONE DEL REGOLAMENTO

36. I codici dovranno precisare l'applicazione pratica del regolamento e rispecchiare in modo accurato la natura dell'attività di trattamento o del settore di trattamento. Essi dovrebbero essere in grado di apportare chiari miglioramenti a livello settoriale in termini di rispetto della normativa in materia di protezione dei dati. I codici dovranno altresì stabilire standard realistici

e conseguibili da tutti gli aderenti e presentare necessariamente una qualità e una coerenza interna tali da apportare un valore aggiunto sufficiente[43]. In altre parole, il progetto di codice dovrà essere adeguatamente focalizzato su particolari aree e questioni relative alla protezione dei dati[44] nel settore specifico cui si applica e dovrà fornire soluzioni sufficientemente chiare ed efficaci con riguardo alle suddette aree e questioni[45].

37. Un codice di condotta non dovrebbe semplicemente parafrasare il regolamento[46]. Dovrebbe invece mirare a codificare in modo specifico, pratico e preciso modalità applicative del regolamento. Le regole e gli standard concordati dovranno essere chiari, concreti, realisticamente conseguibili e applicabili (verificabili). La definizione di regole particolari in un campo specifico è un modo per consentire al codice di costituire un valore aggiunto. L'uso di una terminologia specificamente settoriale e pertinente e la presentazione di casi concreti o di esempi specifici di "migliori prassi"[47] possono contribuire a soddisfare questo requisito[48].

38. Il raggiungimento dell'obiettivo di "precisare l'applicazione del regolamento" può essere facilitato dalla definizione di un programma di promozione del codice approvato così da informare le persone della sua esistenza e del suo contenuto. È fondamentale che i codici siano in grado di dare un significato operativo ai principi di protezione dei dati enunciati all'articolo 5 del regolamento. È inoltre fondamentale che i codici tengano adeguatamente conto delle posizioni e dei pareri pubblicati o approvati dal comitato che rivestono particolare importanza per quel particolare settore o per quella particolare attività di trattamento[49]. Ad esempio, i codici che contengono specifiche relative ad attività di trattamento possono anche facilitare l'individuazione di basi giuridiche adeguate per tali attività negli Stati membri in cui tali codici si applicheranno.

6.4 OFFRE SUFFICIENTI GARANZIE

39. Il codice dovrebbe inoltre soddisfare i requisiti di cui all'articolo 40, paragrafo 5. L'approvazione sarà possibile soltanto quando verrà accertato che il progetto di codice fornisce garanzie sufficienti e adeguate[50]. Il titolare del codice deve dimostrare adeguatamente a un'autorità di controllo competente che tale codice offre garanzie adeguate ed efficaci per mitigare il rischio legato al trattamento dei dati e ai diritti e alle libertà delle persone[51]. Sarà compito dei titolari dei codici dimostrare con chiarezza che il loro codice soddisferà questi requisiti.

> Ad esempio, nel caso di attività di trattamento "ad alto rischio" (quali il trattamento su larga scala di dati relativi a minori o alla salute, la profilazione o il monitoraggio sistematico), il codice dovrebbe contenere obblighi più stringenti per i titolari e i responsabili del trattamento affinché sia garantito un livello di protezione adeguato. Inoltre, i titolari dei codici possono trarre vantaggio da una consultazione più estesa, come previsto

al considerando 99 del regolamento, a supporto di un codice relativo a trattamenti in tali settori ad alto rischio.

6.5 OFFRE MECCANISMI CHE CONSENTIRANNO UN CONTROLLO EFFICACE

40. Ai sensi dell'articolo 40, paragrafo 4, del regolamento, il codice richiede l'attuazione di meccanismi adeguati per garantire che le sue norme siano adeguatamente monitorate e che siano adottate misure di attuazione efficienti e significative per assicurare la piena conformità. Il codice deve, in particolare, identificare e proporre strutture e procedure per monitorare e intervenire efficacemente in caso di violazioni. Il progetto di codice dovrà inoltre identificare un organismo appropriato i cui meccanismi assicurino il monitoraggio efficace del rispetto del codice. Tali meccanismi possono comprendere obblighi regolari di verifica e di segnalazione, procedure chiare e trasparenti di gestione dei reclami e di composizione delle controversie, sanzioni e mezzi di ricorso concreti in caso di violazioni del codice, nonché politiche per segnalare le violazioni delle sue disposizioni.

41. Il progetto di codice deve identificare un organismo di monitoraggio quando contempla attività di trattamento svolte da autorità ed enti non pubblici. Sostanzialmente, il codice non deve solo prevedere il contenuto delle norme applicabili all'attività di trattamento dello specifico settore, ma deve anche attuare meccanismi di monitoraggio che garantiscano l'efficace applicazione di tali norme. Il progetto di codice potrebbe proporre diversi meccanismi di monitoraggio nel caso in cui vi siano più organismi di monitoraggio al fine di effettuare un controllo efficace. Tuttavia, tutti i meccanismi di monitoraggio proposti per monitorare adeguatamente un codice dovranno essere chiari, idonei, realisticamente conseguibili, efficienti e realizzabili (verificabili). I titolari dei codici dovranno esporre il fondamento logico e dimostrare perché le loro proposte di monitoraggio sono adeguate e realizzabili a livello operativo[52].

7. PRESENTAZIONE, AMMISSIBILITÀ E APPROVAZIONE[53] (CODICE NAZIONALE)

7.1 PRESENTAZIONE

42. I titolari del codice devono presentare formalmente il progetto di codice in forma elettronica o in forma scritta (stampata/cartacea) all'autorità di controllo competente[54]. L'autorità di controllo competente ne confermerà la ricezione ai titolari del codice e ne effettuerà un esame per verificare se il progetto di codice soddisfa i criteri di ammissibilità sopra riportati[55] prima di procedere a una valutazione completa del suo contenuto.

7.2 AMMISSIBILITÀ DI UN CODICE

43. Se il progetto di codice non viene accettato perché non soddisfa i criteri di ammissibilità[56] l'autorità di controllo competente risponde per iscritto ai titolari del codice motivando la sua decisione. A questo punto il processo giunge al termine e i titolari del codice dovrebbero effettuare una nuova presentazione[57].

44. Se il progetto di codice soddisfa i criteri di cui sopra, l'autorità di controllo competente dovrebbe confermare per iscritto ai titolari del codice che intende passare alla fase successiva della procedura e valutare il contenuto del progetto di codice nel rispetto delle procedure previste dalla normativa nazionale.

7.3 APPROVAZIONE

45. A meno che il diritto nazionale preveda una tempistica specifica, l'autorità di controllo competente dovrebbe redigere un parere entro un periodo di tempo ragionevole e informare regolarmente i titolari del progetto sullo stato del procedimento e sulla tempistica indicativamente prevista. Il parere deve contenere la motivazione della decisione assunta sulla base dei criteri di approvazione descritti sopra[58].

46. Se l'autorità di controllo competente decide di rifiutare l'approvazione, il processo si conclude e i responsabili dei codici dovranno valutare le conclusioni del parere e, su tale base, riconsiderare il progetto di codice. I responsabili dei codici dovranno inoltre ripresentare formalmente un progetto di codice aggiornato in una fase successiva, se decidono di farlo.

47. Se l'autorità di controllo competente approva il progetto di codice, dovrà registrare e pubblicare il codice (sul suo sito web e/o con altri mezzi di comunicazione appropriati)[59]. L'articolo 40, paragrafo 11, fa inoltre obbligo al comitato di rendere pubblici tutti i codici approvati.

8. PRESENTAZIONE, AMMISSIBILITÀ E APPROVAZIONE[60] (CODICE TRANSNAZIONALE)

8.1 PRESENTAZIONE

48. I titolari del codice devono presentare formalmente il progetto di codice in forma elettronica o in forma scritta a un'autorità di controllo competente, che fungerà da autorità principale per l'approvazione del codice[61]. L'autorità di controllo competente confermerà la ricezione della documentazione ai titolari del codice e ne effettuerà un esame per verificare se il progetto di codice soddisfa i requisiti di cui sopra[62] prima di procedere a una valutazione completa del suo contenuto. L'autorità di controllo competente notifi-

cherà immediatamente a tutte le altre autorità di controllo la presentazione del codice, fornendo i dettagli salienti che ne facilitano l'identificazione e la consultazione. Tutte le autorità di controllo dovranno confermare se siano autorità di controllo interessate, conformemente all'articolo 4, punto 22, lettere a) e b), del regolamento[63].

8.2 AMMISSIBILITÀ DI UN CODICE

49. Se il progetto di codice non viene accettato perché non soddisfa i criteri di ammissibilità di cui sopra, l'autorità di controllo competente comunica per iscritto i motivi della sua decisione ai titolari del codice. Il processo a questo punto giunge al termine e i titolari suddetti dovrebbero effettuare una nuova presentazione[64]. L'autorità di controllo competente trasmette inoltre una notifica per aggiornare tutte le autorità di controllo interessate sulla decisione assunta.
50. Se il progetto di codice viene accettato dall'autorità di controllo competente perché soddisfa i criteri di ammissibilità, l'autorità di controllo competente dovrebbe confermare per iscritto ai titolari del codice che intende passare alla fase successiva della procedura e valutare il contenuto del progetto di codice. Ciò darà il via alla procedura di cooperazione informale descritta di seguito finalizzata a valutare il codice in vista della sua approvazione.

8.3 COOPERAZIONE

51. L'autorità di controllo competente trasmetterà una notifica in cui aggiorna tutte le autorità di controllo[65] in merito alla sua posizione e identifica le autorità di controllo interessate. Essa formulerà inoltre una richiesta di massimo due co-revisori che l'aiutino, su base volontaria, a valutare il contenuto del progetto di codice. La nomina dei co-revisori avverrà secondo il criterio del primo arrivato[66]. Il ruolo dei co-revisori sarà quello di assistere l'autorità di controllo competente nella valutazione del progetto di codice. Una volta confermati i co-revisori, le loro osservazioni sul contenuto del codice dovrebbero essere presentate entro trenta giorni dall'avvenuta conferma. Queste osservazioni verranno quindi prese in considerazione dall'autorità di controllo competente nell'ambito della valutazione da essa condotta ai fini dell'eventuale approvazione. Ai sensi dell'articolo 40, paragrafo 7, del regolamento, l'autorità di controllo competente determinerà in via definitiva se il progetto di decisione debba essere presentato al comitato a norma degli articoli 63 e 64 del regolamento[67].
52. L'autorità di controllo competente dovrebbe prendere una decisione entro un periodo di tempo ragionevole e tenere regolarmente aggiornati i titolari del codice sui progressi e sulla tempistica indicativamente prevista. Dovrebbe motivare la decisione assunta (rigetto o approvazione del codice) in linea con le motivazioni generali per l'approvazione e comunicare tale decisione in modo tempestivo ai titolari del codice.

8.4 RIGETTO

53. Se l'autorità di controllo competente decide di non deferire un progetto di codice al comitato, il processo si conclude. I titolari del codice dovranno quindi analizzare le conclusioni della decisione e valutare una revisione del progetto di codice. I titolari del codice dovrebbero inoltre ripresentarlo per approvazione in una fase successiva, se così ritengono. L'autorità di controllo competente dovrebbe notificare a tutte le autorità di controllo interessate la sua posizione e le motivazioni del rigetto del codice.

8.5 PREPARAZIONE AI FINI DELLA PRESENTAZIONE AL COMITATO

54. Se intende approvare il progetto di codice, l'autorità di controllo competente, prima di sottoporlo al comitato, farà circolare il progetto di approvazione tra tutte le autorità di controllo interessate. Tutte le autorità di controllo interessate avranno 30 giorni per rispondere e qualsiasi questione significativa potrà essere sottoposta per discussione al pertinente sottogruppo del comitato. Se le autorità di controllo interessate non rispondono, il codice passerà alla fase successiva del processo.

8.6 IL COMITATO

55. Se la decisione è di deferire la questione al comitato, conformemente all'articolo 40, paragrafo 7, del regolamento, l'autorità di controllo competente comunicherà tale decisione a tutte le autorità di controllo secondo la procedura del meccanismo di coerenza[68]. L'autorità di controllo competente deferirà inoltre la questione al comitato in linea con il regolamento interno del comitato e con l'articolo 40, paragrafo 7, del regolamento.
56. A norma dell'articolo 64 il comitato rilascerà un parere sulle questioni definite all'articolo 40, paragrafo 7, del regolamento[69]. Al comitato e all'autorità di controllo competente si applicherà il regolamento interno del comitato, insieme al disposto dell'articolo 64, al momento di effettuare una valutazione e di comunicare una decisione sull'approvazione di codici transnazionali.

8.7 APPROVAZIONE

57. Il parere del comitato verrà comunicato all'autorità di controllo competente conformemente all'articolo 64, paragrafo 5, del regolamento e l'autorità di controllo competente dovrà decidere se mantenere o modificare il suo progetto di decisione, conformemente all'articolo 40, paragrafo 5[70]. Il parere del comitato può essere trasmesso anche alla Commissione a norma dell'articolo 40, paragrafo 8, e il comitato, a norma dell'articolo 40, paragrafo 11, raccoglierà tutti i codici transnazionali approvati e li renderà pubblici.

9. COINVOLGIMENTO

58. È importante notare che il processo di valutazione non deve essere un'occasione per proseguire le consultazioni con l'autorità di controllo competente in merito alle disposizioni del codice presentato. A norma dell'articolo 40, paragrafo 5, l'autorità di controllo competente ha il compito di fornire un parere sulla conformità del progetto di codice al regolamento[71]. Pertanto, la comunicazione prevista tra l'autorità di controllo competente e i titolari del codice in questa fase avrà principalmente lo scopo di fare chiarezza e di contribuire a effettuare una valutazione ai sensi degli articoli 40 e 41. Si presume che i titolari del codice interpellino nei modi opportuni le autorità di controllo prima di presentare il progetto di codice per l'approvazione. In linea di principio, la fase di approvazione non dovrebbe stimolare ulteriori consultazioni da parte dei titolari del codice su particolari disposizioni del progetto di codice né dovrebbe consentire un prolungamento delle attività di valutazione a seguito della presentazione di ripetute modifiche all'autorità di controllo competente. È altresì fondamentale che i titolari del codice siano pronti a fornire i chiarimenti richiesti in merito al progetto di codice entro tempi ragionevoli. È importante che i titolari del codice siano preparati e organizzati così da rispondere alle richieste in modo efficiente e competente. Si consiglia di indicare all'autorità di controllo competente un singolo punto di contatto o un apposito referente. Spetterà all'autorità di controllo competente decidere se siano necessarie ulteriori informazioni prima di prendere una decisione sul progetto di codice. Essa potrà inoltre stabilire le modalità di comunicazione tra le parti. Ai fini della continuità, l'autorità di controllo competente resterà anche il principale punto di contatto durante l'intero processo di approvazione dei codici transnazionali.

10. IL RUOLO DELLA COMMISSIONE

59. La Commissione può decidere, mediante atti di esecuzione, che un codice transnazionale approvato ha validità generale all'interno dell'Unione e, in tal caso, provvede a darvi un'adeguata pubblicità[72].

11. MONITORAGGIO DI UN CODICE

60. Affinché un codice (nazionale o transnazionale) sia approvato, occorre che tale codice individui un organismo (o più organismi) di monitoraggio e che tale organismo (o tali organismi) siano accreditati dall'autorità di controllo competente in quanto capaci di monitorare efficacemente il codice[73]. L'autorità di controllo competente presenterà al comitato il progetto di requisiti per l'accreditamento di un organismo di monitoraggio, ai sensi del meccanismo di coerenza di cui all'articolo 63 del regolamento. Una volta approvati dal comitato, i requisiti possono quindi essere applicati dall'autorità di controllo competente per accreditare un organismo di monitoraggio.

61. Il regolamento non definisce il termine "accreditamento". Tuttavia, l'articolo 41, paragrafo 2, del regolamento delinea i requisiti generali per l'accreditamento dell'organismo di monitoraggio. Vi sono diversi requisiti che devono essere soddisfatti per convincere l'autorità di controllo competente ad accreditare un organismo di monitoraggio. I titolari del codice dovranno spiegare e dimostrare in che modo l'organismo di monitoraggio da essi proposto soddisfa i requisiti di cui all'articolo 41, paragrafo 2, per ottenerne l'accreditamento.

62. Il regolamento ammette una certa flessibilità in merito alla natura e alla struttura dell'organismo di monitoraggio da accreditare ai sensi dell'articolo 41. I titolari del codice possono decidere di utilizzare organismi di monitoraggio esterni o interni, purché in entrambi i casi l'organismo in questione soddisfi i requisiti di accreditamento di cui all'articolo 41, paragrafo 2, come meglio descritti di seguito.

12. REQUISITI DI ACCREDITAMENTO PER GLI ORGANISMI DI MONITORAGGIO

12.1 INDIPENDENZA

63. I titolari del codice dovranno dimostrare che l'organismo in questione è adeguatamente indipendente (in termini di imparzialità di funzioni) dagli aderenti al codice e dalla professione o dal settore di attività cui si applica il codice. L'indipendenza può essere dimostrata a vari livelli quali: il finanziamento dell'organismo di monitoraggio, la nomina dei membri/del personale, il processo decisionale e, più in generale, la struttura organizzativa. Questi aspetti vengono esaminati più avanti in maggior dettaglio.

64. Esistono due principali modelli di monitoraggio utilizzabili dai titolari del codice per soddisfare i requisiti relativi all'organismo di monitoraggio: organismo di monitoraggio esterno ovvero organismo di monitoraggio interno. Nell'ambito di questi due modelli di monitoraggio è ammessa una certa flessibilità e sono proponibili versioni diverse, adeguate al contesto del codice. Quali esempi di organismi di monitoraggio interni si possono citare un comitato interno ad hoc o un dipartimento indipendente e distinto all'interno della struttura del titolare del codice. Spetterà a quest'ultimo spiegare l'approccio in materia di gestione dei rischi per quanto riguarda imparzialità e indipendenza dell'organismo.

65. Ad esempio, qualora sia proposto un organismo di monitoraggio interno, il personale, la dirigenza, la responsabilità e le funzioni dovrebbero essere separati dalle altre aree dell'organizzazione. Ciò può essere conseguito in vari modi, ad esempio utilizzando efficaci barriere organizzative e informative, e distinte strutture di riporto gerarchico per l'associazione e per l'organismo di monitoraggio. Analogamente a un responsabile della protezione dei dati, l'organismo di monitoraggio deve essere in grado di agire senza ricevere istruzioni e deve essere protetto da qualsiasi tipo di sanzione o interferenza (diretta o indiretta) conseguente all'adempimento dei suoi compiti.

66. Il requisito dell'indipendenza potrebbe comportare la necessità, per un consulente esterno o un altro soggetto coinvolto nella stesura del codice di condotta, di dimostrare l'esistenza di garanzie adeguate così da attenuare sufficientemente il rischio relativo all'indipendenza o un conflitto di interessi. L'organismo di monitoraggio dovrebbe fornire elementi atti a dimostrare l'adeguatezza dei meccanismi intesi a identificare e a ridurre tali rischi in modo soddisfacente[74]. L'organismo di monitoraggio dovrà identificare i rischi per la sua imparzialità su base continua, nelle sue attività o nei suoi rapporti. Se viene identificato un rischio per l'imparzialità, l'organismo di monitoraggio dovrebbe dimostrare in che modo elimina o riduce tale rischio e come utilizza un meccanismo adeguato al fine di salvaguardare la propria imparzialità.
67. Un altro indice di indipendenza potrebbe essere rappresentato dalla dimostrazione di una piena autonomia nella gestione del bilancio e di altre risorse, in particolare nel caso di un organismo di monitoraggio interno. L'indipendenza dell'organismo di monitoraggio dovrebbe manifestarsi anche nella scelta e nell'applicazione delle sanzioni nei confronti di un titolare o di un responsabile del trattamento che aderisce al codice. In sostanza, l'organismo (interno o esterno) dovrà agire in modo indipendente dai titolari del codice e dagli aderenti a quest'ultimo quando assolve i suoi compiti ed esercita i suoi poteri.

12.2 CONFLITTO DI INTERESSI[75]

68. Occorre dimostrare che l'adempimento dei compiti e delle funzioni dell'organismo di monitoraggio non dà adito a conflitto di interessi. I titolari del codice dovranno quindi dimostrare che l'organismo di monitoraggio proposto si asterrà da qualunque azione incompatibile con i suoi compiti e con le sue funzioni, e che sono state predisposte garanzie per assicurare che l'organismo non eserciti alcuna altra attività incompatibile. Allo stesso modo, l'organismo di monitoraggio non deve subire pressioni esterne, né dirette, né indirette, e non sollecita né accetta istruzioni da alcuna persona, organizzazione o associazione. L'organismo dovrebbe disporre di proprio personale, scelto dall'organismo stesso o da un altro organismo indipendente previsto dal codice, e soggetto unicamente all'autorità di tali organismi. Nel caso di un organismo di monitoraggio interno, esso deve essere protetto da qualsiasi tipo di sanzione o interferenza (diretta o indiretta) da parte del titolare del codice, di altri organismi competenti[76] o degli aderenti al codice, conseguente all'adempimento dei suoi compiti.

12.3 COMPETENZE

69. I titolari del codice devono essere in grado di dimostrare che l'organismo di monitoraggio possiede il livello necessario di competenze per svolgere la

propria funzione in modo efficace. Pertanto, la presentazione del progetto di codice dovrà includere dettagli sulle conoscenze e sulle esperienze acquisite dall'organismo nell'ambito della normativa sulla protezione dei dati nonché rispetto al particolare settore o alla particolare attività di trattamento. Ad esempio, la dimostrabilità di esperienze pregresse in ruoli di monitoraggio per un particolare settore può contribuire a soddisfare questo requisito. Inoltre, saranno gradite una comprensione approfondita delle problematiche inerenti alla protezione dei dati e una conoscenza specialistica dei trattamenti oggetto del codice. Il personale dell'organismo di monitoraggio proposto dovrebbe avere maturato anche un'adeguata esperienza operativa e avere ricevuto un'adeguata formazione in materia di monitoraggio della conformità, ad esempio nell'ambito di attività di verifica, monitoraggio o assicurazione della qualità.

12.4 PROCEDURE E STRUTTURE CONSOLIDATE

70. L'organismo di monitoraggio dovrà inoltre disporre di appropriate strutture e procedure di governance, che gli consentano di effettuare in maniera adeguata quanto segue:

- valutare l'idoneità di titolari e responsabili del trattamento ad applicare il codice;
- monitorare il rispetto delle disposizioni del codice, e
- riesaminare periodicamente il funzionamento del codice.

71. Si dovrebbero elaborare procedure di controllo complete per valutare adeguatamente l'idoneità di titolari e responsabili del trattamento a sottoscrivere e a rispettare il codice. L'organismo di monitoraggio dovrebbe inoltre garantire che le disposizioni del codice possano essere soddisfatte dai titolari e dai responsabili del trattamento.

72. Saranno necessarie procedure e strutture per monitorare attivamente ed efficacemente il rispetto del codice da parte degli aderenti, quali verifiche con o senza preavviso, ispezioni annuali, relazioni periodiche e l'uso di questionari[77]. Le procedure di monitoraggio possono essere strutturate in modi diversi purché tengano conto di fattori quali i rischi legati ai trattamenti oggetto del codice, i reclami ricevuti o gli incidenti specifici, il numero di aderenti al codice, ecc.. Si potrebbe valutare la pubblicazione delle relazioni di verifica nonché tenere conto dei risultati di relazioni periodiche presentate dai titolari e dai responsabili del trattamento soggetti al codice.

73. I titolari del codice dovranno anche dimostrare che l'organismo di monitoraggio proposto dispone di risorse e personale adeguati a svolgere i compiti affidatigli. Le risorse dovrebbero essere proporzionate al numero previsto di aderenti al codice e alle rispettive dimensioni, nonché alla complessità o al livello di rischio del trattamento in questione.

12.5 GESTIONE TRASPARENTE DEI RECLAMI

74. L'organismo di monitoraggio dovrà istituire procedure e strutture efficaci che permettano di gestire i reclami in modo trasparente e imparziale. A tal fine esso dovrà adottare un processo di gestione dei reclami accessibile al pubblico, dotato di risorse sufficienti per gestire i reclami e per garantire che le decisioni dell'organismo siano rese disponibili al pubblico.

> La dimostrazione dell'esistenza di una procedura di gestione dei reclami potrebbe consistere, ad esempio, nella descrizione di un processo di ricezione, valutazione, tracciamento, registrazione e risoluzione dei reclami. Tale descrizione potrebbe figurare in una guida al codice accessibile al pubblico, che permetta al reclamante di comprendere e seguire la procedura di gestione dei reclami. Inoltre, l'indipendenza di tali processi potrebbe essere facilitata separando il personale operativo dalle funzioni direttive all'interno dell'organismo di monitoraggio.

75. L'organismo di monitoraggio dovrebbe inoltre disporre di procedure efficaci per garantire il rispetto del codice da parte dei titolari o dei responsabili del trattamento. Ad esempio si potrebbe conferire all'organismo di monitoraggio il potere di sospendere o di escludere dal codice un titolare o un responsabile del trattamento che non rispetti le regole del codice (ossia, conferendo il potere di imporre misure correttive).

76. Se un aderente al codice ne viola le regole, l'organismo di monitoraggio è tenuto a prendere immediatamente le debite misure. L'obiettivo di tali idonee misure correttive sarà quello di porre termine alla violazione e di evitare che si ripeta in futuro. Tali azioni correttive e sanzioni potrebbero comprendere un'ampia gamma di misure quali obblighi di formazione, una comunicazione di messa in mora, la segnalazione del titolare o del responsabile al comitato, un avviso formale con la richiesta di implementare azioni specifiche entro una determinata data, la sospensione temporanea dal codice fino all'adozione di misure correttive, e in ultima analisi l'esclusione definitiva dal codice. Queste misure potrebbero essere divulgate dall'organismo di monitoraggio, soprattutto in caso di gravi violazioni del codice.

77. Laddove necessario, l'organismo di monitoraggio dovrebbe essere in grado di informare il singolo aderente, il titolare del codice, l'autorità di controllo competente e tutte le autorità di controllo interessate in merito alle misure adottate e alle rispettive motivazioni, senza ingiustificato ritardo[78]. Inoltre, nel caso in cui sia identificabile un'autorità di controllo capofila[79] per un aderente a un codice transnazionale, l'organismo di monitoraggio dovrebbe opportunamente informare anche quest'ultima sulle azioni intraprese.

12.6 COMUNICAZIONE CON L'AUTORITÀ DI CONTROLLO COMPETENTE

78. Le disposizioni relative all'organismo di monitoraggio nella proposta di codice devono prevedere che tale organismo comunichi efficacemente all'autorità di controllo competente e ad altre autorità di controllo tutte le attività svolte con riguardo al codice, fra cui le decisioni sulle misure adottate in caso di violazione del codice da parte di un aderente, la presentazione di relazioni periodiche sul codice, la presentazione dei risultati di un riesame o di una verifica del codice[80].

79. Deve essere inoltre garantito che l'espletamento delle funzioni dell'autorità di controllo non sia pregiudicato od ostacolato. Ad esempio, un codice che preveda la possibilità per gli aderenti di approvare, revocare o sospendere unilateralmente un organismo di monitoraggio senza alcuna notifica e accordo con l'autorità di controllo competente violerebbe l'articolo 41, paragrafo 5, del regolamento.

12.7 MECCANISMI DI RIESAME

80. Il codice deve definire opportuni meccanismi di riesame che gli consentano di mantenere la propria attualità e di continuare a contribuire alla corretta applicazione del regolamento. Si dovrebbero prevedere meccanismi di riesame anche per adeguare il codice a eventuali modifiche a livello di applicazione e interpretazione delle norme o qualora nuovi sviluppi tecnologici possano incidere sul trattamento dei dati effettuato dagli aderenti o sulle disposizioni del codice.

12.8 STATUS GIURIDICO

81. L'organismo di monitoraggio proposto (interno o esterno) e le strutture di governance collegate dovranno essere concepiti in modo da consentire ai titolari del codice di dimostrare che l'organismo di monitoraggio dispone di uno status giuridico adeguato a svolgere la sua funzione ai sensi dell'articolo 41, paragrafo 4, ed è passibile di sanzioni ai sensi dell'articolo 83, paragrafo 4, lettera c), del regolamento.

13. CODICI APPROVATI

82. Chiaramente, saranno la natura e il contenuto del codice a definire i ruoli dei soggetti interessati per quanto riguarda la garanzia del rispetto del codice e del regolamento. Tuttavia, l'autorità di controllo competente avrà sempre un ruolo da svolgere nel garantire l'idoneità del codice rispetto agli obiettivi in esso definiti.

83. L'autorità di controllo competente lavorerà quindi a stretto contatto con l'organismo di monitoraggio in rapporto agli obblighi di segnalazione derivanti dal codice. L'organismo di monitoraggio sarà il referente e il coordinatore principale per eventuali problematiche che potrebbero insorgere in relazione al codice.

84. L'autorità di controllo competente dovrebbe inoltre approvare le eventuali ulteriori modifiche o proroghe del codice e accreditare eventuali nuovi organismi di monitoraggio[81]. Ai sensi dell'articolo 40, paragrafo 5, del regolamento, qualsiasi modifica o proroga di un codice esistente dovrà essere sottoposta a un'autorità di controllo competente in linea con le procedure descritte nel presente documento.

14. REVOCA DI UN ORGANISMO DI MONITORAGGIO

85. Quando un organismo di monitoraggio non rispetta le disposizioni applicabili del regolamento, l'autorità di controllo competente avrà anche il potere di revocarne l'accreditamento ai sensi dell'articolo 41, paragrafo 5[82]. È importante che il titolare del codice preveda disposizioni adeguate in caso di revoca.

86. Tuttavia, la revoca dell'accreditamento dell'unico organismo di monitoraggio previsto in un codice può comportare la sospensione o la revoca permanente del codice, in quanto viene a mancare il necessario controllo della conformità. Ciò può influire negativamente sulla reputazione o sugli interessi commerciali degli aderenti al codice e può deprimere la fiducia degli interessati o di altri soggetti.

87. Se le circostanze lo permettono, la revoca dovrebbe avvenire soltanto dopo che l'autorità di controllo competente ha dato all'organismo di monitoraggio l'opportunità di affrontare urgentemente le problematiche o di apportare gli opportuni miglioramenti entro un termine concordato. Quando si tratti di codici transnazionali, l'autorità di controllo competente, prima di concordare con l'organismo di monitoraggio termini specifici per la gestione delle problematiche evidenziate, dovrebbe interpellare in merito le autorità di controllo interessate. La decisione di revocare un organismo di monitoraggio dovrebbe essere comunicata a tutte le autorità di controllo interessate e al comitato (ai sensi dell'articolo 40, paragrafo 11).

15. CODICI DEL SETTORE PUBBLICO

88. L'articolo 41, paragrafo 6, del regolamento prevede che il monitoraggio dei codici di condotta approvati non si applichi al trattamento effettuato da autorità pubbliche o da organismi pubblici[83]. Sostanzialmente questa disposizione elimina il requisito del monitoraggio del codice da parte di un organismo accreditato, ma non riduce in alcun modo l'obbligo di mettere in atto mec-

canismi efficaci per monitorare un codice. A tal fine è possibile modificare requisiti esistenti in materia di audit così da includervi il monitoraggio del codice.

Per il comitato europeo per la protezione dei dati
La presidente

(Andrea Jelinek)

APPENDICE 1 - DISTINZIONE TRA CODICI NAZIONALI E TRANSNAZIONALI

Un codice transnazionale è un codice che disciplina le attività di trattamento in più di uno Stato membro. Un codice transnazionale può quindi riguardare attività di trattamento svolte da una molteplicità di titolari o di responsabili del trattamento in vari Stati membri senza configurare necessariamente un "trattamento transfrontaliero" nei termini di cui all'articolo 4, paragrafo 23, del regolamento.

Pertanto, se un codice di condotta adottato da un'associazione nazionale di uno Stato membro si applica alle attività di trattamento svolte dai suoi aderenti in diversi Stati membri, esso si qualificherà come un codice transnazionale.

Per contro, se un'associazione con un codice approvato a livello nazionale accetta l'adesione di un membro internazionale che svolge trattamenti transfrontalieri, tale membro potrà far valere il codice approvato soltanto per le attività di trattamento svolte nello Stato membro che ha approvato il codice[84]. Si dovrebbero predisporre meccanismi volti a garantire un'adeguata trasparenza in ordine all'effettivo ambito di applicazione territoriale del codice.

APPENDICE 2 - SCEGLIERE L'AUTORITÀ DI CONTROLLO COMPETENTE

I titolari dei codici sono liberi di scegliere l'autorità di controllo competente cui chiedere l'approvazione del loro progetto di codice transnazionale[85]. Il regolamento non prevede regole specifiche per identificare l'autorità di controllo competente più adatta a svolgere la valutazione di un progetto di codice. Tuttavia, per aiutare i titolari dei codici a identificare l'autorità di controllo competente più idonea a valutare il loro codice, si riportano di seguito alcuni fattori di cui eventualmente tenere conto[86]:

- il luogo in cui l'attività di trattamento o il settore di trattamento presenta la maggiore densità;
- il luogo con la maggiore densità di interessati oggetto dell'attività o del settore di trattamento;
- il luogo in cui ha la sede principale il titolare del codice;
- il luogo in cui ha la sede principale l'organismo di monitoraggio proposto;
- le iniziative sviluppate da un'autorità di controllo in un campo specifico[87].

Benché questi fattori non siano criteri prescrittivi, la scelta dell'autorità di controllo competente è importante e va effettuata con prudenza[88]. Il ruolo dell'autorità di controllo competente comprende, tra l'altro, la funzione di punto di contatto unico per i titolari dei codici durante il processo di approvazione, la gestione della procedura nella fase di cooperazione, l'accreditamento dell'organismo di monitoraggio (se del caso) e la funzione di capofila delle attività di vigilanza al fine dell'efficace monitoraggio del codice approvato.

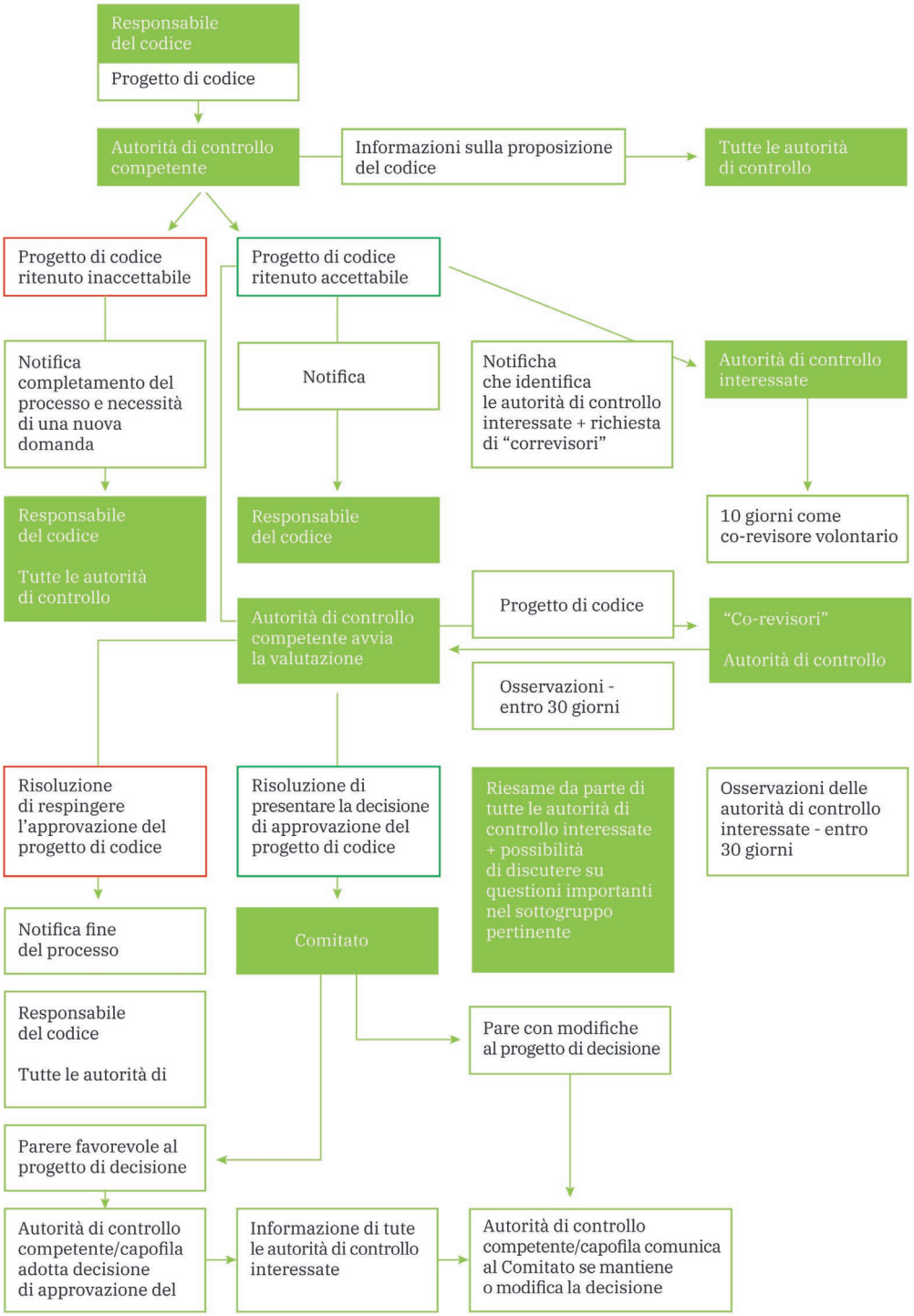
APPENDICE 3 - LISTA DI CONTROLLO PER LA PRESENTAZIONE

Prima di presentare un progetto di codice all'autorità di controllo competente è importante assicurarsi di avere accluso o definito i seguenti elementi (ove applicabili) segnalandoli adeguatamente all'interno della documentazione:

1. Avete fornito una motivazione e tutta la pertinente documentazione di supporto? (punto 20)
2. Siete un'associazione o un'altra organizzazione che rappresenta categorie di titolari o di responsabili del trattamento? (punto 21)
3. Nella presentazione avete fornito gli elementi utili a dimostrare di essere un organismo rappresentativo efficace, capace di comprendere le esigenze dei membri? (punto 22)
4. Avete definito chiaramente l'attività o il settore di trattamento e i problemi di trattamento di cui il codice intende occuparsi? (punto 23)
5. Avete identificato l'ambito di applicazione territoriale del codice e incluso un elenco di tutte le autorità di controllo interessate (ove applicabile)? (punto 24)
6. Avete fornito elementi atti a giustificare la scelta dell'autorità di controllo competente? (punto 25)
7. Avete incluso meccanismi che consentono un monitoraggio efficace del rispetto del codice? (punto 26)
8. Avete identificato un organismo di monitoraggio e spiegato come esso soddisferà i requisiti di monitoraggio del codice? (punto 27)
9. Avete incluso informazioni sull'entità delle consultazioni svolte in fase di sviluppo del codice? (punto 28)
10. Avete confermato che il progetto di codice è conforme alla normativa dello Stato membro (ove applicabile)? (punto 29)
11. Avete soddisfatto i requisiti linguistici? (punto 30)

La vostra presentazione include elementi sufficienti a dimostrare la corretta applicazione del regolamento? (punti 32-41)

APPENDICE 4 - DIAGRAMMA DI FLUSSO PER UN CODICE TRANSNAZIONALE



NOTE

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[2] Cfr. il considerando 13 del regolamento.

[3] Cfr. l'articolo 5, paragrafo 2, del regolamento.

[4] Cfr. ad esempio l'articolo 24, paragrafo 3, l'articolo 28, paragrafo 5, e l'articolo 32, paragrafo 3. Un codice di condotta può anche essere utilizzato dal responsabile del trattamento per dimostrare garanzie sufficienti che il trattamento soddisfa i requisiti del regolamento (si veda l'articolo 28, paragrafo 5).

[5] Cfr. i considerando 77, 81, 98, 99, 148, 168 e gli articoli 24, 28, 35, 40, 41, 46, 57, 64 e 70 del regolamento. Ciò vale in particolare quando un codice si riferisce ad attività di trattamento in diversi Stati membri.

[6] I codici non devono necessariamente essere circoscritti o limitati a un settore specifico. Ad esempio, un codice potrebbe applicarsi a settori distinti che però condividono un'attività di trattamento con le stesse caratteristiche ed esigenze. Nel caso in cui un codice sia di applicazione intersettoriale, possono essere designati più organismi di monitoraggio per quello stesso codice. Tuttavia, in tal caso, il codice dovrebbe chiarire senza ombra di dubbio la portata delle funzioni di ciascun organismo di monitoraggio, ossia specificando i settori per i quali ciascun organismo di monitoraggio svolgerà le sue funzioni ai sensi dell'articolo 41 e i meccanismi di vigilanza a disposizione di ciascun organismo. A tal proposito, le pertinenti sezioni delle presenti linee guida che definiscono le responsabilità, gli obblighi e i requisiti di accreditamento in relazione agli organismi di monitoraggio si applicano a ciascuno di tali organismi designati con riguardo a un determinato codice.

[7] Articolo 40, paragrafo 1, del regolamento.

[8] Cfr. l'articolo 40, paragrafo 5, l'articolo 55, paragrafo 1 e il considerando 122 del regolamento.

[9] Cfr. l'articolo 40, paragrafo 1, e il considerando 98 del regolamento.

[10] Cfr. ad esempio l'articolo 41, paragrafo 2, e l'articolo 41, paragrafo 3, del regolamento.

[11] Dalle autorità nazionali di controllo o dal gruppo di lavoro "Articolo 29" prima dell'adozione del regolamento e delle presenti linee guida.

[12] Un organismo di monitoraggio può tuttavia essere accreditato per più di un codice, purché soddisfi i requisiti per l'accreditamento.

[13] In conformità del considerando 98 del regolamento.

[14] Cfr. anche i successivi punti 64-67.

[15] I codici di condotta e la certificazione sono strumenti di responsabilizzazione volontari, mentre la valutazione d'impatto sulla protezione dei dati in alcune circostanze è obbligatoria. Per ulteriori informazioni su altri strumenti di responsabilizzazione si rimanda alla pagina web contenente orientamenti generali del comitato (www.edpb.europa.eu).

[16] Cfr. l'articolo 42 del regolamento e le linee guida 1/2018 del comitato sulla certificazione e sull'identificazione dei criteri di certificazione a norma degli articoli 42 e 43 del regolamento

[17] L'adesione a un codice non garantisce di per sé la conformità al regolamento né l'immunità del titolare del trattamento/responsabile del trattamento da sanzioni o responsabilità previste dal regolamento.

[18] Cfr. il considerando 98 del regolamento riguardo all'articolo 40, paragrafo 1. Ad esempio, un codice potrebbe essere opportunamente adattato per soddisfare le esigenze delle micro-organizzazioni oltre che delle piccole e medie imprese.

[19] L'articolo 40, paragrafo 1, del regolamento, in particolare, identifica i codici come una soluzione per soddisfare le esigenze di tali imprese.

[20] L'articolo 40, paragrafo 2, del regolamento fa riferimento a codici elaborati da organizzazioni rappresentative delle "categorie di titolari del trattamento o responsabili del trattamento". Ciò potrebbe pertanto includere codici intersettoriali, a condizione che i criteri di rappresentatività siano rispettati.

[21] Un codice più specifico deve esplicitare in misura sufficientemente chiara agli interessati (e

a giudizio di un'autorità di controllo competente) che l'adesione al codice da parte dei titolari del trattamento/responsabili del trattamento non garantisce necessariamente il rispetto di tutta la legislazione. Un'opportuna misura di salvaguardia in questo caso potrebbe essere quella di assicurare un'adeguata trasparenza rispetto alla portata limitata del codice sia a coloro che vi hanno aderito sia agli interessati.

[22] Cfr. l'articolo 40, paragrafo 2, lettera j), e l'articolo 40, paragrafo 3, del regolamento.

[23] Il comitato elaborerà distinte linee guida riguardo all'uso dei codici come strumento per facilitare i trasferimenti internazionali.

[24] Cfr. anche l'articolo 24, paragrafo 3, e l'articolo 28, paragrafo 5, del regolamento.

[25] Articolo 32, paragrafo 3, del regolamento.

[26] Articolo 35, paragrafo 8, del regolamento.

[27] Articolo 83, paragrafo 2, lettera j), del regolamento. Si veda anche l'applicazione di codici di condotta in relazione alle linee guida WP 253/17 riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) 2016/679, adottate dal comitato.

[28] *Ibidem*

[29] Valevole anche per tutti i codici (nazionali e transnazionali) e i codici modificati o prorogati.

[30] Per esempio, in via non esaustiva: identificazione degli aderenti, attività di trattamento, interessati, tipologie di dati, giurisdizioni, autorità di controllo interessate (articolo 4, punto 22, del regolamento).

[31] Con questo documento i titolari del codice possono dimostrare la ratio alla base dell'approvazione richiesta. È uno strumento che consente ai titolari del codice di illustrare l'adeguatezza delle garanzie proposte e di dimostrare che i meccanismi proposti sono adatti allo scopo.

[32] Ad esempio una sintesi delle consultazioni, informazioni sulle adesioni o ricerche che dimostrino la necessità del codice.

[33] Ai sensi dell'articolo 55 del regolamento ogni autorità di controllo è competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti a norma del regolamento nel territorio del rispettivo Stato membro. Cfr. anche il considerando 122.

[34] Cfr. l'articolo 40, paragrafo 4, del regolamento.

[35] Un codice rivolto al settore pubblico dovrà comunque prevedere meccanismi adeguati per il suo monitoraggio.

[36] A norma dell'articolo 83, paragrafo 4, lettera c), del regolamento, la violazione degli obblighi di un organismo di monitoraggio è soggetta a una sanzione amministrativa pecuniaria.

[37] Cfr. la sezione "Requisiti di accreditamento per gli organismi di monitoraggio" a pagina 24.

[38] I titolari del codice potrebbero ad esempio spiegare come hanno valutato le proposte ricevute a seguito della consultazione.

[39] La normativa nazionale di alcuni Stati membri potrebbe prescrivere di presentare il progetto di codice nella lingua nazionale; si raccomanda ai titolari del codice di esaminare la questione con l'autorità di controllo competente prima di presentare formalmente il progetto di codice per l'approvazione.

[40] L'inglese è la lingua di lavoro del comitato a norma dell'art. 23 del suo regolamento interno.

[41] Ad esempio, nei settori ad "alto rischio", come il trattamento dei dati riguardanti i minori o la salute, si dovrebbero prevedere garanzie più solide e stringenti, vista la sensibilità dei dati personali in questione.

[42] Cfr. l'articolo 40, paragrafo 1, del regolamento.

[43] Questo criterio è stato applicato per la prima volta nel documento WP 13 DG XV D/5004/98, adottato il 10 settembre 1998.

[44] Come quelle di cui all'articolo 40, paragrafo 2, del regolamento.

[45] Questo requisito riflette la posizione del Gruppo di lavoro "Articolo 29", illustrata nel documento di lavoro relativo ai codici WP 13 DG XV D/5004/98, adottato il 10 settembre 1998.

[46] La parafrasi della normativa in materia di protezione dei dati era un tratto caratterizzante i progetti di codice di condotta sottoposti senza esito positivo all'approvazione del gruppo di lavoro "Articolo 29".

[47] E di "pratiche inaccettabili".

[48] Il codice dovrebbe evitare, ove possibile, l'uso di formule giuridiche involute.

[49] Dovranno inoltre tenere pienamente conto della pertinente giurisprudenza nazionale ed europea.

[50] Cfr. il considerando 98 del regolamento.

[51] Queste garanzie possono anche applicarsi agli organismi di monitoraggio e alla capacità di svolgere le rispettive funzioni in maniera efficace.

[52] Anche il documento del gruppo di lavoro "Articolo 29" "Valutazione dell'autoregolamen-

tazione dell'industria: quando reca un contributo significativo al livello di protezione dei dati in un paese terzo?" WP7, adottato il 14 gennaio 1998, è un documento informativo che offre ulteriori dettagli sulla determinazione del valore di un codice e sui presupposti che ne determinano l'efficacia. Al momento di formulare il codice è consigliabile prendere in esame anche questo documento (se del caso).

[53] Incluse la modifica e la proroga di codici precedentemente approvati.

[54] Ovviamente tale autorità sarà l'autorità di controllo nazionale per gli aderenti al codice cui quest'ultimo si applica. È importante, inoltre, che i titolari del codice indichino con chiarezza all'autorità di controllo competente che stanno presentando formalmente un progetto di codice per l'approvazione e che specifichino chiaramente l'ambito di applicazione del codice. Si veda anche l'appendice 1 per quanto riguarda la differenza tra i codici nazionali e transnazionali.

[55] Si veda anche la lista di controllo di cui all'appendice 3.

[56] *Ibidem*

[57] Occorre notare che il rigetto, in questa fase del processo di approvazione, dipenderà molto probabilmente dalla non conformità a requisiti preliminari generali o procedurali piuttosto che da questioni sostanziali o fondamentali legate alle disposizioni contenute nel progetto di codice.

[58] In questo modo l'autorità di controllo competente può fornire osservazioni utili ai titolari del codice qualora decidano di rivedere, modificare e ripresentare un progetto di codice in un momento successivo

[59] Conformemente all'articolo 40, paragrafo 6, del regolamento.

[60] Incluse la modifica e la proroga di codici precedentemente approvati.

[61] Questa indicazione deve essere letta alla luce della procedura descritta di seguito.

[62] Si veda anche la lista di controllo di cui all'appendice 3.

[63] Ciò è importante in quanto si prevede che i co-revisori del progetto di codice siano autorità di controllo interessate dal trattamento dei dati personali perché il titolare o il responsabile del trattamento è stabilito nel territorio dello Stato membro di tale autorità di controllo o perché "gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento".

[64] Occorre notare che il rigetto, in questa fase del processo di approvazione, dipenderà molto probabilmente dalla non conformità a requisiti preliminari generali o procedurali piuttosto che da questioni sostanziali o fondamentali legate alle disposizioni contenute nel progetto di codice.

[65] Le autorità di controllo interessate dovrebbero essere identificabili in base all'ambito di applicazione del progetto di codice.

[66] Questa richiesta resterà aperta per dieci giorni lavorativi. In attesa dell'individuazione dei co-revisori, l'autorità di controllo competente procederà con la valutazione. Di norma, l'autorità di controllo competente si consulterà con due co-revisori quando il codice interessa 14 Stati membri o più. Sotto questa soglia è possibile avere uno o due co-revisori, a seconda dei casi.

[67] Il che può verificarsi solo qualora l'autorità di controllo competente intenda approvare il progetto di codice. Cfr. l'articolo 40, paragrafo 7 e l'articolo 64, paragrafo 1, del regolamento.

[68] Si veda l'articolo 64, paragrafo 4, del regolamento, secondo il quale si dovrebbero presentare i pareri di altre autorità di controllo interessate insieme al progetto di decisione dell'autorità di controllo competente.

[69] Si veda il compito del comitato di cui all'articolo 70, paragrafo 1, lettera x), del regolamento.

[70] Si vedano l'articolo 64, paragrafo 7, e le procedure invocate nel caso in cui un'autorità di controllo competente non concordi con il parere del comitato conformemente all'articolo 64, paragrafo 8, del regolamento.

[71] L'autorità di controllo competente può anche fornire indicazioni e, se del caso, formulare raccomandazioni ai titolari del codice in merito al contenuto e al formato del progetto di codice.

[72] Cfr. l'articolo 40, paragrafo 9 e l'articolo 40, paragrafo 10, del regolamento. Tale decisione consentirebbe inoltre ai titolari e ai responsabili del trattamento che non sono soggetti al regolamento di assumere impegni vincolanti e azionabili riguardo a un codice convalidato (cfr. l'articolo 40, paragrafo 3). Ciò consentirebbe trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali sulla base dell'esistenza di garanzie adeguate e della disponibilità di diritti azionabili e mezzi di ricorso effettivi per gli interessati (si vedano anche l'articolo 46, paragrafo 1 e l'articolo 46, paragrafo 2, lettera e)).

[73] Articolo 41, paragrafo 1, del regolamento. Si noti anche che l'articolo 41 non si applica alle autorità pubbliche o agli organismi pubblici.

[74] Il contesto del codice determinerà l'approccio da adottare. Ad esempio, può essere suffi-

ciente che nel progetto di codice vi sia un'adeguata separazione delle funzioni, da cui risulti che il personale dell'organismo di monitoraggio non ha redatto né testato il codice.

[75] Imparzialità di funzione, ossia la capacità di agire autonomamente.

[76] Organismi rappresentativi di categorie di titolari o di responsabili del trattamento.

[77] In questo modo si potrebbe anche evitare che alcuni aderenti siano controllati ripetutamente, a differenza di altri.

[78] Se il monitoraggio viene effettuato da un organismo esterno all'associazione/all'organizzazione che presenta il codice di condotta, anche il titolare del codice dovrebbe essere informato.

[79] Ai sensi dell'articolo 56 del regolamento.

[80] Si veda l'articolo 41, paragrafo 4.

[81] Fra le modifiche che richiedono l'approvazione, ad esempio, potrebbe rientrare l'aggiunta di una nuova norma al codice, ma non l'aggiornamento del riferimento al nome di un'organizzazione o altre modifiche minori che non incidono sul funzionamento del codice.

[82] Per i codici transnazionali è fondamentale anche che l'autorità di controllo competente si assicuri che tutte le autorità di controllo interessate siano informate di questo provvedimento. In modo analogo, per tali codici, un'autorità di controllo interessata dovrebbe informare l'autorità di controllo competente anche nei casi in cui un titolare del trattamento (teoricamente aderente al codice) risulti esservi inadempiente, poiché tale informazione potrebbe gettare ombre sull'efficacia dell'organismo di monitoraggio e del codice.

[83] La classificazione delle autorità o degli organismi del settore pubblico spetta al singolo Stato membro.

[84] Tuttavia, utilizzando lo stesso esempio, i titolari del codice potrebbero anche valutare di estenderne l'ambito di applicazione e chiedere l'approvazione di un codice transnazionale.

[85] Cfr. l'articolo 55 e il considerando 122 del regolamento.

[86] L'elenco non è in ordine gerarchico né è esaustivo.

[87] Ad esempio, un'autorità di controllo potrebbe avere pubblicato un documento orientativo dettagliato e significativo, che fa diretto riferimento all'attività di trattamento oggetto del codice.

[88] Una richiesta di approvazione di un progetto di codice non può essere rigettata da un'autorità di controllo competente sulla base del mancato rispetto di alcuni o della totalità dei criteri non esaustivi di cui all'appendice 2. Una tale richiesta può essere rigettata soltanto se non sono rispettati i criteri indicati nella sezione "Ammissibilità di un progetto di codice".

Torna a **Indice** | **Premessa**

Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati - Versione 2.0

8 ottobre 2019

Cronologia delle versioni

Versione 2.0	8 ottobre 2019	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	9 aprile 2019	Adozione delle linee guida per la consultazione pubblica

Indice

1 Parte 1 - Introduzione
- 1.1 Contesto
- 1.2 Oggetto delle presenti linee guida

2 Parte 2 - Analisi dell'articolo 6, paragrafo 1, lettera b)
- 2.1 Osservazioni generali
- 2.2 Interazione dell'articolo 6, paragrafo 1, lettera b) con altri fondamenti di liceità del trattamento
- 2.3 Ambito di applicazione dell'articolo 6, paragrafo 1, lettera b)
- 2.4 Necessità
- 2.5 Necessario all'esecuzione di un contratto stipulato con l'interessato
- 2.6 Risoluzione del contratto
- 2.7 Necessario all'esecuzione di misure precontrattuali

3 Parte 3 - Applicabilità dell'articolo 6, paragrafo 1, lettera b), in situazioni specifiche
- 3.1 Trattamento per finalità di «miglioramento dei servizi»
- 3.2 Trattamento per finalità di «prevenzione delle frodi»
- 3.3 Trattamento per finalità di pubblicità comportamentale online
- 3.4 Trattamento per finalità di personalizzazione dei contenuti

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

1. PARTE 1 - INTRODUZIONE

1.1 CONTESTO

1. A norma dell'articolo 8 della Carta dei diritti fondamentali dell'Unione europea, i dati personali devono essere trattati in modo corretto, per finalità determinate e in base a un fondamento legittimo previsto dalla legge. A tale riguardo, l'articolo 6, paragrafo 1, del regolamento generale sulla protezione dei dati[1] (RGPD) stabilisce che il trattamento è lecito soltanto sulla base di una delle sei condizioni specificate di cui all'articolo 6, paragrafo 1, lettere da a) a f). L'individuazione della base giuridica appropriata corrispondente all'obiettivo e all'essenza del trattamento è di fondamentale importanza. Nell'individuare la base legittima appropriata, i titolari del trattamento devono tenere conto anche dell'impatto sui diritti degli interessati in maniera da rispettare il principio di correttezza.
2. L'articolo 6, paragrafo 1, lettera b) del RGPD configura un fondamento di liceità per il trattamento di dati personali nella misura in cui «il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso»[2]. Ciò sostiene la libertà d'impresa, garantita dall'articolo 16 della Carta, e riflette il fatto che talvolta non è possibile ottemperare alle obbligazioni contrattuali nei confronti dell'interessato senza che quest'ultimo fornisca determinati dati personali. Se il trattamento specifico è parte integrante dell'erogazione del servizio richiesto, il trattamento di tali dati è nell'interesse di entrambe le parti poiché altrimenti non sarebbe possibile fornire il servizio e dare esecuzione al contratto. Tuttavia, la possibilità di ricorrere a questa o a una delle altre basi giuridiche di cui all'articolo 6, paragrafo 1, non esenta il titolare del trattamento dall'osservanza degli altri requisiti previsti dal RGPD.
3. Gli articoli 56 e 57 del Trattato sul funzionamento dell'Unione europea definiscono e disciplinano la libera prestazione dei servizi all'interno dell'Unione europea. Sono state adottate misure legislative specifiche dell'UE per quanto concerne i «servizi della società dell'informazione»[3]. Tali servizi sono definiti come «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica [...] e a richiesta individuale di un destinatario di servizi». Questa definizione si estende ai servizi che non sono pagati direttamente dalle persone che li ricevono[4], come i servizi online finanziati mediante la pubblicità. Il termine «servizi online», come utilizzato nelle presenti linee guida, si riferisce ai «servizi della società dell'informazione».
4. Lo sviluppo del diritto dell'Unione riflette l'importanza fondamentale dei servizi online nella società moderna. La diffusione di Internet sempre attivo sui dispositivi mobili e l'ampia disponibilità di dispositivi connessi hanno consentito lo sviluppo di servizi online in settori quali i *social media*, il commercio elettronico, la ricerca su Internet, la comunicazione e i viaggi. Mentre taluni di questi servizi sono finanziati dai pagamenti degli utenti, altri sono forniti senza un corrispettivo monetario da parte del consumatore essendo invece finanziati dalla vendita di servizi pubblicitari online che permettono

di rivolgersi in maniera mirata agli interessati. Il tracciamento del comportamento degli utenti ai fini di tale pubblicità è di frequente effettuato secondo modalità ignote all'utente[5]; inoltre, tale attività può non essere immediatamente evidente in ragione della natura del servizio fornito, circostanza questa che rende praticamente impossibile all'interessato l'esercizio di una scelta informata sull'utilizzo dei propri dati.

5. In questo contesto, il comitato europeo per la protezione dei dati[6] (EDPB) ritiene opportuno fornire orientamenti sull'applicabilità dell'articolo 6, paragrafo 1, lettera b), al trattamento di dati personali nel contesto dei servizi online, al fine di garantire che tale fondamento di liceità sia invocato soltanto ove opportuno.

6. Il Gruppo di lavoro «Articolo 29» (WP29) si è già espresso sulla base giuridica costituita dalla necessità del trattamento per scopi contrattuali ai sensi della direttiva 95/46/CE nel suo parere sul concetto di interesse legittimo del titolare del trattamento[7]. In generale, tali orientamenti restano pertinenti per quanto concerne l'articolo 6, paragrafo 1, lettera b), e il RGPD.

1.2 OGGETTO DELLE PRESENTI LINEE GUIDA

7. Le presenti linee guida riguardano l'applicabilità dell'articolo 6, paragrafo 1, lettera b), al trattamento di dati personali nel contesto di contratti per servizi online, indipendentemente dalle modalità di finanziamento dei servizi. Le linee guida illustreranno gli elementi di liceità del trattamento ai sensi dell'articolo 6, paragrafo 1, lettera b), del RGPD e prenderanno in esame la nozione di «necessità» in quanto riferita al trattamento «necessario all'esecuzione di un contratto».

8. Le norme in materia di protezione dei dati disciplinano aspetti importanti delle modalità di interazione dei servizi online con gli utenti, tuttavia non sono le uniche norme applicabili. La regolamentazione dei servizi online comporta responsabilità interfunzionali nei settori, tra l'altro, del diritto dei consumatori e del diritto in materia di concorrenza. Le considerazioni relative a questi settori del diritto esulano dall'oggetto delle presenti linee guida.

9. Sebbene l'articolo 6, paragrafo 1, lettera b), possa applicarsi soltanto in un contesto contrattuale, le presenti linee guida non si pronunciano sulla validità in generale dei contratti relativi ai servizi online, in quanto ciò non rientra nelle competenze del comitato europeo per la protezione dei dati. Tuttavia i contratti e le clausole contrattuali devono essere conformi ai requisiti del diritto contrattuale e, se del caso per i contratti conclusi dai consumatori, alla normativa che tutela i consumatori, affinché il trattamento basato su tali clausole possa essere considerato corretto e lecito.

10. Di seguito sono riportate talune osservazioni generali sui principi in materia di protezione dei dati, tuttavia non saranno esaminate tutte le questioni relative alla protezione dei dati che possono emergere durante il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettera b). I titolari del tratta-

mento devono sempre garantire il rispetto dei principi di protezione dei dati di cui all'articolo 5 e di tutti gli altri requisiti del RGPD nonché, se del caso, della legislazione relativa alla tutela della vita privata nel settore delle comunicazioni elettroniche.

2. PARTE 2 - ANALISI DELL'ARTICOLO 6, PARAGRAFO 1, LETTERA B)

2.1 OSSERVAZIONI GENERALI

11. Il fondamento di liceità del trattamento di cui all'articolo 6, paragrafo 1, lettera b), va considerato nel contesto complessivo del RGPD, degli obiettivi di cui all'articolo 1 di quest'ultimo e dell'obbligo dei titolari di trattare i dati personali nel rispetto dei principi di protezione dei dati di cui all'articolo 5. Ciò comprende un trattamento corretto e trasparente dei dati personali che sia in linea con il principio di limitazione delle finalità e gli obblighi di minimizzazione dei dati.
12. L'articolo 5, paragrafo 1, lettera a), del RGPD stabilisce che i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Il principio di correttezza comprende, tra l'altro, il riconoscimento delle ragionevoli aspettative[8] degli interessati, la considerazione di eventuali conseguenze negative per gli interessati a causa del trattamento e la valutazione del rapporto fra interessati e titolare del trattamento nonché degli effetti potenzialmente derivanti da squilibri in tale rapporto.
13. Come menzionato, in termini di liceità, i contratti relativi ai servizi online devono essere validi ai sensi del diritto contrattuale applicabile. Un esempio significativo al riguardo è dato dalla circostanza per cui l'interessato sia un minore. In tal caso (e al di là del rispetto dei requisiti del RGPD, comprese le misure di «specifica protezione» che si applicano ai minori)[9], il titolare del trattamento deve garantire la conformità alle leggi nazionali pertinenti in materia di capacità negoziale dei minori. Inoltre, al fine di garantire il rispetto dei principi di correttezza e liceità, il titolare del trattamento deve soddisfare altri requisiti giuridici. Ad esempio, per i contratti conclusi da consumatori, può essere applicabile la direttiva 93/13/CEE concernente le clausole abusive nei contratti stipulati con i consumatori («direttiva sulle clausole abusive nei contratti»)[10]. L'articolo 6, paragrafo 1, lettera b), non si limita ai contratti disciplinati dalla legge di uno Stato membro del SEE[11].
14. L'articolo 5, paragrafo 1, lettera b), del RGPD stabilisce il principio della limitazione delle finalità, che impone che i dati personali siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.
15. L'articolo 5, paragrafo 1, lettera c) del medesimo regolamento prevede il principio della minimizzazione dei dati, ossia il trattamento del minor volume di dati possibile per il conseguimento della specifica finalità. Questa valutazione integra le valutazioni della necessità del trattamento di cui all'ar-

ticolo 6, paragrafo 1, lettere da b) ad f).

16. Tanto il principio della limitazione della finalità quanto quello della minimizzazione dei dati sono particolarmente pertinenti nei contratti per i servizi online che di norma non sono negoziati individualmente. I progressi tecnologici consentono ai titolari del trattamento di raccogliere e trattare facilmente un quantitativo di dati personali superiore a quanto mai accaduto in passato. Di conseguenza sussiste l'elevato rischio che i titolari cerchino di includere nei contratti clausole generali di trattamento al fine di massimizzare la raccolta e gli utilizzi possibili dei dati, senza specificarne adeguatamente le finalità o tenere conto degli obblighi di minimizzazione dei dati. Come già affermato dal Gruppo di lavoro «Articolo 29»:

    La finalità della raccolta deve essere indicata in maniera chiara e specifica: deve essere sufficientemente dettagliata da consentire di stabilire quale tipo di trattamento è incluso nella finalità specifica e quale no, nonché da consentire di valutare il rispetto della legge e l'applicazione delle garanzie in materia di protezione dei dati. Per questi motivi, una finalità che sia vaga o generica, come ad esempio «migliorare l'esperienza degli utenti», «finalità di marketing», «finalità di sicurezza informatica» o «ricerca futura», senza ulteriori dettagli, di solito non soddisfa i criteri di specificità.[12]

2.2 INTERAZIONE DELL'ARTICOLO 6, PARAGRAFO 1, LETTERA B) CON ALTRI FONDAMENTI DI LICEITÀ DEL TRATTAMENTO

17. Se il trattamento non è considerato «necessario all'esecuzione di un contratto», ossia quando un servizio richiesto può essere prestato senza lo svolgimento del trattamento specifico, il comitato europeo per la protezione dei dati riconosce che può essere applicabile un'altra base giuridica, purché siano soddisfatte le condizioni pertinenti. In particolare, in determinate circostanze, può essere più opportuno basarsi sul consenso liberamente espresso ai sensi dell'articolo 6, paragrafo 1, lettera a). In altri casi, l'articolo 6, paragrafo 1, lettera f), può costituire un fondamento di liceità più idoneo per il trattamento. La base giuridica deve essere individuata prima dell'attuazione del trattamento e deve essere specificata nelle informazioni fornite agli interessati conformemente agli articoli 13 e 14.

18. È possibile che un'altra base giuridica, diversa dall'articolo 6, paragrafo 1, lettera b), possa corrispondere meglio all'obiettivo e al contesto del trattamento in questione. L'individuazione della base giuridica appropriata è legata ai principi di correttezza e limitazione delle finalità[13].

19. Le linee guida del Gruppo di lavoro «Articolo 29» in materia di consenso chiariscono altresì che quando «il titolare del trattamento intende trattare dati personali che sono effettivamente necessari per l'esecuzione di un contratto il consenso non è la base legittima appropriata». Per altro verso, il comitato europeo per la protezione dei dati ritiene che, se il trattamento non è effettivamente necessario all'esecuzione di un contratto, tale trattamento può avvenire soltanto sul fondamento di un'altra base giuridica appropriata[14].

20. Nel rispetto degli obblighi in materia di trasparenza, i titolari del trattamento dovrebbero assicurarsi di evitare qualsiasi confusione riguardo alla base giuridica applicabile. Ciò è particolarmente importante quando la base giuridica appropriata è l'articolo 6, paragrafo 1, lettera b), e gli interessati stipulano un contratto relativo a servizi online. A seconda delle circostanze, gli interessati possono erroneamente avere l'impressione di esprimere un consenso in linea con l'articolo 6, paragrafo 1, lettera a), firmando un contratto o accettando condizioni di servizio. Al tempo stesso, un titolare del trattamento potrebbe erroneamente presumere che la firma di un contratto corrisponda a una manifestazione di consenso ai sensi dell'articolo 6, paragrafo 1, lettera a). Si tratta di concetti assolutamente diversi. È importante distinguere tra l'accettazione di condizioni di servizio ai fini della conclusione di un contratto e la prestazione di un consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), dato che tali concetti hanno requisiti e conseguenze giuridiche diversi.

21. Per quanto concerne il trattamento di categorie particolari di dati personali, nelle linee guida sul consenso il Gruppo di lavoro «Articolo 29» ha osservato altresì che:

    L'articolo 9, paragrafo 2, non riconosce il trattamento «necessario all'esecuzione di un contratto» come un'eccezione al divieto generale di trattare categorie particolari di dati. Di conseguenza i titolari del trattamento e gli Stati membri che rientrano nel contesto di applicazione di tale circostanza dovrebbero esaminare le eccezioni specifiche di cui all'articolo 9, paragrafo 2, lettere da b) a j). Qualora non si applichi nessuna delle eccezioni da b) a j), l'ottenimento del consenso esplicito in conformità con le condizioni per il consenso valido previste dal regolamento rimane l'unica eccezione lecita possibile per trattare tali dati[15].

2.3 AMBITO DI APPLICAZIONE DELL'ARTICOLO 6, PARAGRAFO 1, LETTERA B)

22. L'articolo 6, paragrafo 1, lettera b) si applica quando è soddisfatta une delle seguenti due condizioni: il trattamento in questione deve essere oggettivamente necessario all'esecuzione di un contratto stipulato con l'interessato, oppure il trattamento deve essere oggettivamente necessario al fine di attuare misure precontrattuali su richiesta di un interessato.

2.4 NECESSITÀ

23. La necessità del trattamento è un prerequisito per entrambe le condizioni di cui all'articolo 6, paragrafo 1, lettera b). Innanzitutto, è importante osservare che la nozione di ciò che è «necessario all'esecuzione di un contratto» non equivale alla semplice valutazione di ciò che è consentito o previsto nelle clausole di un contratto. La nozione di necessità ha un significato autonomo nel diritto dell'Unione europea, che deve rispecchiare gli obiettivi della normativa in materia di protezione dei dati[16]. Di conseguenza occorre tene-

re conto anche del diritto fondamentale alla tutela della vita privata e alla protezione dei dati personali[17], nonché dei requisiti stabiliti dai principi in materia di protezione dei dati e, in particolare, dal principio di correttezza.

24. Il punto di partenza consiste quindi nell'individuare la finalità del trattamento e, nel contesto di una relazione contrattuale, possono esservi molteplici finalità di trattamento. Tali finalità devono essere chiaramente specificate e comunicate all'interessato, nel rispetto degli obblighi di limitazione delle finalità e di trasparenza cui il titolare del trattamento è soggetto.

25. La valutazione di ciò che è «necessario» comporta una valutazione combinata, basata sui fatti, del trattamento «per l'obiettivo perseguito e della possibilità che tale trattamento sia meno intrusivo rispetto ad altre opzioni disponibili per il conseguimento del medesimo obiettivo»[18]. Laddove esistano alternative realistiche e meno invasive, il trattamento non è «necessario»[19]. L'articolo 6, paragrafo 1, lettera b), non si applicherà al trattamento che è utile, ma non oggettivamente necessario per eseguire il servizio oggetto del contratto o per adottare le pertinenti misure precontrattuali su richiesta dell'interessato, anche laddove ciò sia necessario per altre finalità commerciali del titolare del trattamento.

2.5 NECESSARIO ALL'ESECUZIONE DI UN CONTRATTO STIPULATO CON L'INTERESSATO

26. Un titolare del trattamento può invocare la prima opzione di cui all'articolo 6, paragrafo 1, lettera b), per trattare dati personali quando può stabilire, nel rispetto dei propri obblighi in materia di responsabilizzazione di cui all'articolo 5, paragrafo 2, sia che il trattamento ha luogo nel contesto di un contratto valido stipulato con l'interessato sia che il trattamento è necessario ai fini dell'esecuzione di tale specifico contratto concluso con l'interessato. Qualora un titolare non sia in grado di dimostrare a) l'esistenza di un contratto, b) la validità del contratto ai sensi del diritto contrattuale nazionale applicabile e c) l'oggettiva necessità del trattamento ai fini dell'esecuzione del contratto, tale titolare dovrebbe prendere in considerazione un'altra base giuridica per il trattamento.

27. Un mero riferimento al trattamento dei dati o la semplice menzione di tale trattamento in un contratto non è sufficiente a far rientrare il trattamento in questione nell'ambito di applicazione dell'articolo 6, paragrafo 1, lettera b). Al contrario, il trattamento può essere oggettivamente necessario anche se non espressamente menzionato nel contratto. In ogni caso, il titolare del trattamento deve adempiere i propri obblighi in materia di trasparenza. Qualora un titolare intenda stabilire che il trattamento si fonda sull'esecuzione di un contratto stipulato con l'interessato, è importante valutare ciò che è *oggettivamente necessario* ai fini dell'esecuzione del contratto. Il concetto di «necessario all'esecuzione» richiede chiaramente qualcosa di più di una clausola contrattuale. Ciò è evidente anche alla luce dell'articolo 7, paragrafo 4. Sebbene tale disposizione riguardi soltanto la validità del consenso, essa opera,

a titolo esemplificativo, una distinzione tra le attività di trattamento necessarie all'esecuzione di un contratto e le clausole che subordinano l'erogazione del servizio a talune attività di trattamento che di fatto non sono necessarie ai fini dell'esecuzione del contratto.

28. A tale riguardo il comitato europeo per la protezione dei dati avalla gli orientamenti precedentemente adottati dal Gruppo di lavoro «Articolo 29» sulla disposizione equivalente di cui alla precedente direttiva, secondo la quale la nozione di «necessario all'esecuzione di un contratto stipulato con l'interessato»:

    [...] deve essere interpretata rigorosamente e non contempla le situazioni in cui il trattamento non è effettivamente necessario all'esecuzione di un contratto, bensì imposto unilateralmente all'interessato dal [titolare] del trattamento. Inoltre, il fatto che alcuni trattamenti di dati siano coperti da un contratto non significa automaticamente che tali trattamenti siano necessari alla sua esecuzione. [...] Anche se tali attività di trattamento sono espressamente menzionate in caratteri minuscoli nel contratto, questo fatto, da solo, non le rende «necessarie» all'esecuzione del contratto[20].

29. Il comitato europeo per la protezione dei dati ricorda inoltre che negli stessi orientamenti del Gruppo di lavoro «Articolo 29» si afferma che:

    In questo caso esiste un chiaro collegamento tra la valutazione della necessità e il rispetto del principio di limitazione delle finalità. È importante stabilire la ratio esatta del contratto, ossia la sua sostanza e il suo obiettivo fondamentale, poiché sarà questa la base su cui si valuterà se il trattamento dei dati è necessario alla sua esecuzione[21].

30. Nel valutare se l'articolo 6, paragrafo 1, lettera b), costituisca una base giuridica appropriata per il trattamento nel contesto di un servizio contrattuale online, si dovrebbe tener conto dello scopo, della finalità o dell'obiettivo specifico/a del servizio. Ai fini dell'applicabilità dell'articolo 6, paragrafo 1, lettera b), è necessario che il trattamento sia *oggettivamente necessario* per una finalità che è parte integrante della prestazione di tale servizio contrattuale all'interessato. Il trattamento dei dati relativi al pagamento ai fini dell'addebito del servizio non è escluso da tale contesto. Il titolare del trattamento dovrebbe essere in grado di dimostrare in che modo l'oggetto principale del c*ontratto specifico stipulato con l'interessato* non sia di fatto realizzabile senza lo specifico trattamento dei dati personali in questione. Essenziale in questo contesto è il nesso tra i dati personali e i trattamenti in questione, nonché l'esecuzione o meno del servizio reso ai sensi del contratto.

31. I contratti relativi a servizi digitali possono comprendere termini espliciti che impongono, tra l'altro, condizioni aggiuntive in materia di pubblicità, pagamenti o cookie. Un contratto non può ampliare artificiosamente le categorie di dati personali o le tipologie di trattamenti che il titolare necessita di effettuare per l'esecuzione del contratto ai sensi dell'articolo 6, paragrafo 1, lettera b).

32. Il titolare del trattamento dovrebbe essere in grado di giustificare la necessità di tale trattamento avendo riguardo all'oggetto essenziale del contratto come inteso da entrambe le parti. A questo scopo si dovrà tenere conto non soltanto del punto di vista del titolare del trattamento, ma anche della ra-

gionevole valutazione compiuta dall'interessato al momento della stipula del contratto e della possibilità di ritenere che l'"esecuzione" del contratto abbia luogo comunque anche in assenza del trattamento in questione. Sebbene il titolare del trattamento possa ritenere che il trattamento sia necessario per la finalità contrattuale, è importante che esamini attentamente il punto di vista di un interessato medio, al fine di garantire un'effettiva intesa reciproca in merito alla finalità del contratto.

33. Ai fini della valutazione dell'applicabilità dell'articolo 6, paragrafo 1, lettera b), possono risultare utili le domande riportate di seguito:

- qual è la natura del servizio fornito all'interessato? quali sono le sue caratteristiche distintive?
- qual è la *ratio* esatta del contratto (ossia la sua sostanza e il suo oggetto fondamentale)?
- quali sono gli elementi essenziali del contratto?
- quali sono le prospettive e le aspettative reciproche delle parti contraenti? Come viene promosso o pubblicizzato il servizio all'interessato? Un utente medio del servizio potrebbe ragionevolmente aspettarsi che, tenuto conto della natura del servizio stesso, il trattamento previsto abbia luogo per l'esecuzione del contratto di cui è parte?

34. Se la valutazione di ciò che è «necessario all'esecuzione di un contratto», che deve essere condotta prima di dare corso al trattamento, dimostra che il trattamento previsto va al di là di quanto oggettivamente necessario per l'esecuzione di un contratto, ciò non rende tale futuro trattamento illecito di per sé. Come già menzionato, l'articolo 6 chiarisce che esistono potenzialmente altre basi giuridiche sulle quali fare affidamento prima dell'inizio del trattamento[22].

35. Se, durante il ciclo di vita di un servizio, vengono introdotte nuove tecnologie che modificano le modalità di trattamento dei dati personali oppure il servizio evolve in altro modo, occorre valutare nuovamente i criteri di cui sopra per stabilire se eventuali trattamenti nuovi o modificati possano trovare fondamento nell'articolo 6, paragrafo 1, lettera b).

Esempio 1

Un interessato acquista dei prodotti da un rivenditore al dettaglio online. L'interessato vuole pagare con carta di credito e desidera che i prodotti gli vengano consegnati al proprio domicilio. Al fine di soddisfare il contratto, tale rivenditore deve trattare le informazioni della carta di credito e l'indirizzo di fatturazione dell'interessato per finalità di pagamento, nonché l'indirizzo di residenza dell'interessato per effettuare la consegna. Di conseguenza l'articolo 6, paragrafo 1, lettera b), è applicabile come base giuridica a tali attività di trattamento.

Tuttavia se il cliente ha optato per la spedizione presso un punto di ritiro, il trattamento dell'indirizzo di residenza dell'interessato non è più neces-

necessario per l'esecuzione del contratto di acquisto. Qualsiasi trattamento dell'indirizzo dell'interessato in questo contesto richiederà l'applicazione di una base giuridica diversa rispetto all'articolo 6, paragrafo 1, lettera b).

Esempio 2

Il medesimo rivenditore al dettaglio online intende creare profili dei gusti e delle scelte in termini di stile di vita degli utenti, basati sulle loro visite sul sito web. Il perfezionamento del contratto di acquisto non dipende dalla creazione di tali profili. Anche qualora la profilazione sia espressamente menzionata nel contratto, ciò di per sé non rende la profilazione «necessaria» all'esecuzione del contratto. Se il rivenditore al dettaglio online desidera effettuare tale profilazione, deve fare affidamento su una base giuridica diversa.

36. Nel contesto del diritto contrattuale e, se del caso, della normativa in materia di tutela dei consumatori, i titolari del trattamento sono liberi di progettare i propri servizi, contratti e attività commerciali. In taluni casi un titolare del trattamento potrebbe voler raggruppare più servizi separati o elementi di un servizio con finalità, caratteristiche o ratio differenti in un unico contratto. Ciò può creare una situazione del tipo «prendere o lasciare» per quegli interessati che intendono usufruire soltanto di uno dei servizi.

37. Dal punto di vista del diritto in materia di protezione dei dati, i titolari del trattamento devono tenere conto del fatto che le attività di trattamento previste devono fondarsi su una base giuridica appropriata. Se il contratto è costituito da più servizi distinti o da più elementi di un servizio distinti che di fatto possono ragionevolmente essere svolti indipendentemente l'uno dall'altro, si pone la questione circa la misura in cui l'articolo 6, paragrafo 1, lettera b), possa fungere da base giuridica. L'applicabilità dell'articolo 6, paragrafo 1, lettera b), dovrebbe essere valutata nel contesto di ciascuno di tali servizi separatamente, considerando ciò che è oggettivamente necessario per ciascuno dei singoli servizi che l'interessato ha attivamente richiesto o sottoscritto. Tale valutazione può rivelare che certune attività di trattamento non sono necessarie per i singoli servizi richiesti dall'interessato, quanto piuttosto per il modello aziendale complessivo del titolare del trattamento. In tal caso l'articolo 6, paragrafo 1, lettera b), non costituirà una base giuridica per quelle attività. Tuttavia possono essere disponibili altre basi giuridiche per i trattamenti in questione, come l'articolo 6, paragrafo 1, lettera a) o f), a condizione che siano soddisfatti i criteri pertinenti. Di conseguenza la valutazione dell'applicabilità dell'articolo 6, paragrafo 1, lettera b), non incide sulla legittimità del contratto o del raggruppamento di servizi in quanto tale.

38. Come rilevato in precedenza dal Gruppo di lavoro «Articolo 29», la base giuridica si applica soltanto a ciò che è necessario all'esecuzione di un contratto[23].

Di conseguenza non si applica automaticamente a tutte le ulteriori azioni innescate da un'inosservanza o da qualsiasi altro incidente nell'esecuzione di un contratto. Tuttavia talune azioni possono essere ragionevolmente previste e necessarie nel contesto di una normale relazione contrattuale, come ad esempio l'invio di solleciti formali in merito a pagamenti scaduti oppure la correzione di errori o ritardi nell'esecuzione del contratto. L'articolo 6, paragrafo 1, lettera b) può disciplinare un trattamento di dati personali necessario in relazione a tali azioni.

Esempio 3

Una società vende prodotti online. Il cliente contatta la società perché il colore del prodotto acquistato è diverso da quello concordato. Il trattamento dei dati personali del cliente al fine di rettificare tale aspetto può fondarsi sull'articolo 6, paragrafo 1, lettera b).

39. La garanzia contrattuale può rientrare nell'esecuzione di un contratto e quindi la conservazione di taluni dati per un periodo specificato successivamente al perfezionamento dello scambio di beni/servizi o del pagamento ai fini della garanzia contrattuale può essere necessaria all'esecuzione di un contratto.

2.6 RISOLUZIONE DEL CONTRATTO

40. Un titolare del trattamento deve individuare la base giuridica appropriata per le operazioni di trattamento previste prima dell'inizio del trattamento. Qualora l'articolo 6, paragrafo 1, lettera b), costituisca il fondamento giuridico di talune o della totalità delle attività di trattamento, il titolare dovrebbe prevedere le conseguenze in caso di risoluzione del contratto[24].
41. Qualora il trattamento di dati personali sia basato sull'articolo 6, paragrafo 1, lettera b) e il contratto sia risolto totalmente, in linea di massima il trattamento di tali dati non sarà più necessario per l'esecuzione del contratto e di conseguenza il titolare del trattamento dovrà cessare l'attività di trattamento. L'interessato potrebbe aver fornito i propri dati personali nel contesto di una relazione contrattuale confidando nel fatto che i dati sarebbero stati trattati esclusivamente per quanto necessario nell'ambito di tale relazione. Di conseguenza, in linea di principio, è scorretto passare a una nuova base giuridica una volta che quella originaria cessi di esistere.
42. In caso di risoluzione di un contratto, possono rendersi necessarie determinate attività amministrative come la restituzione di beni o di un pagamento. Il trattamento associato può basarsi sull'articolo 6, paragrafo 1, lettera b).
43. L'articolo 17, paragrafo 1, lettera a), prevede che i dati personali vengano cancellati quando non sono più necessari per le finalità per le quali sono stati raccolti. Questa disposizione non si applica se il trattamento è necessario per

determinate finalità, fra cui il rispetto di un obbligo legale ai sensi dell'articolo 17, paragrafo 3, lettera b) oppure l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria ai sensi dell'articolo 17, paragrafo 3, lettera e). Nella pratica, se i titolari del trattamento ritengono necessario conservare informazioni per le finalità di cui sopra, devono individuare una base giuridica per tale eventualità sin dall'inizio del trattamento e devono comunicare chiaramente fin dall'inizio per quanto tempo intendono conservare le informazioni per tali finalità dopo la risoluzione del contratto. Qualora procedano in tal senso, non sono tenuti a cancellare i dati al momento della risoluzione del contratto.

44. In ogni caso, è possibile che siano stati individuati preliminarmente più trattamenti aventi finalità e basi giuridiche distinte. Finché tali altri trattamenti rimangono leciti e il titolare ha fornito informazioni chiare in materia all'inizio del trattamento, in linea con gli obblighi di trasparenza previsti dal RGPD, rimarrà possibile trattare i dati personali relativi all'interessato per tali finalità distinte anche successivamente alla risoluzione del contratto.

Esempio 4

Un servizio online fornisce un servizio in abbonamento che può essere annullato in qualsiasi momento. Al momento della stipula di un contratto per tale servizio il titolare del trattamento fornisce informazioni all'interessato in merito al trattamento di dati personali.

Il titolare del trattamento spiega, tra l'altro, che, in vigenza del contratto, egli tratterà i dati relativi all'utilizzo del servizio per emettere fatture. La base giuridica applicabile è l'articolo 6, paragrafo 1, lettera b), in quanto il trattamento per finalità di fatturazione può essere considerato oggettivamente necessario per l'esecuzione del contratto. Tuttavia in caso di risoluzione del contratto e supponendo che non vi siano contenziosi pendenti o obblighi giuridici di conservazione dei dati, la cronologia relativa all'utilizzo dovrà essere cancellata.

Inoltre il titolare del trattamento informa gli interessati di essere soggetto a un obbligo di legge ai sensi del diritto interno che gli impone di conservare determinati dati personali per finalità contabili per un certo numero di anni. La base giuridica appropriata è l'articolo 6, paragrafo 1, lettera c) e la conservazione avverrà anche in caso di risoluzione del contratto.

2.7 NECESSARIO ALL'ESECUZIONE DI MISURE PRECONTRATTUALI

45. La seconda opzione offerta dall'articolo 6, paragrafo 1, lettera b), si applica quando il trattamento è *necessario all'esecuzione* di misure precontrattuali prese su *richiesta dell'interessato*. Questa disposizione rispecchia il fatto che può essere necessario effettuare un trattamento preliminare di dati personali prima della conclusione di un contratto al fine di facilitare l'effettiva stipula dello stesso.

46. Al momento del trattamento non è sempre chiaro se si giungerà o meno alla stipula di un contratto. La seconda opzione di cui all'articolo 6, paragrafo 1, lettera b), può comunque essere applicata purché l'interessato presenti la richiesta nel contesto della *potenziale* conclusione di un contratto e il trattamento in questione sia necessario per l'esecuzione delle misure precontrattuali richieste. Pertanto, qualora un interessato contatti il titolare del trattamento per chiedere informazioni circa i dettagli delle offerte di servizi di tale titolare, il trattamento dei dati personali dell'interessato ai fini della risposta alla richiesta di informazioni può basarsi sull'articolo 6, paragrafo 1, lettera b).

47. In ogni caso questa disposizione non si applica all'invio di materiale pubblicitario non richiesto o ad altri trattamenti effettuati esclusivamente su iniziativa del titolare o su richiesta di una terza parte.

Esempio 5

Un interessato fornisce il proprio codice postale per sapere se il prestatore di un determinato servizio opera nella propria zona. Ciò può essere considerato un trattamento necessario all'esecuzione di misure precontrattuali su richiesta dell'interessato ai sensi dell'articolo 6, paragrafo 1, lettera b).

Esempio 6

In taluni casi gli istituti finanziari sono tenuti a identificare i loro clienti ai sensi del diritto interno. Ai fini del rispetto di tale obbligo, prima di concludere un contratto con gli interessati, una banca chiede loro di esibire i documenti di identità.

In questo caso, l'identificazione è necessaria in virtù di un obbligo legale cui la banca è soggetta piuttosto che ai fini dell'esecuzione di misure precontrattuali su richiesta dell'interessato. Di conseguenza la base giuridica appropriata non è l'articolo 6, paragrafo 1, lettera b), bensì l'articolo 6, paragrafo 1, lettera c).

3. PARTE 3 – APPLICABILITÀ DELL'ARTICOLO 6, PARAGRAFO 1, LETTERA B), IN SITUAZIONI SPECIFICHE

3.1 TRATTAMENTO PER FINALITÀ DI «MIGLIORAMENTO DEI SERVIZI»[25]

48. Spesso i servizi online raccolgono informazioni dettagliate sulle modalità di interazione degli utenti con il loro servizio. Nella maggior parte dei casi, la raccolta di dati relativi a parametri organizzativi concernenti un servizio o di dettagli relativi al coinvolgimento degli utenti non può essere considerata necessaria per la prestazione del servizio, in quanto il servizio può essere

fornito in assenza del trattamento di tali dati personali. Tuttavia un prestatore di servizi può fondare tale trattamento su basi giuridiche alternative quali il legittimo interesse o il consenso.

49. Il comitato europeo per la protezione dei dati non ritiene che l'articolo 6, paragrafo 1, lettera b), costituisca in via generale una base giuridica appropriata per un trattamento svolto ai fini del miglioramento di un servizio o dello sviluppo di nuove funzioni nel contesto di un servizio esistente. Nella maggior parte dei casi, un utente stipula un contratto per avvalersi di un servizio esistente. Sebbene la possibilità di apportare miglioramenti e modifiche a un servizio sia spesso sistematicamente inclusa nei termini contrattuali, tale trattamento non può essere considerato oggettivamente necessario, in via generale, all'esecuzione del contratto stipulato con l'utente.

3.2 TRATTAMENTO PER FINALITÀ DI «PREVENZIONE DELLE FRODI»

50. Come rilevato in precedenza dal Gruppo di lavoro «Articolo 29»[26], il trattamento per finalità di prevenzione delle frodi può comportare il monitoraggio e la profilazione dei clienti. Secondo il comitato europeo per la protezione dei dati è probabile che tale trattamento ecceda quanto oggettivamente necessario all'esecuzione di un contratto stipulato con un interessato. Tuttavia il trattamento dei dati personali strettamente necessario per finalità di prevenzione delle frodi può costituire un legittimo interesse del titolare del trattamento[27] e può quindi essere considerato lecito se il titolare soddisfa i requisiti specifici di cui all'articolo 6, paragrafo 1, lettera f) (legittimo interesse). Inoltre, anche l'articolo 6, paragrafo 1, lettera c) (osservanza di un obbligo legale) potrebbe costituire una base giuridica per il trattamento in questione.

3.3 TRATTAMENTO PER FINALITÀ DI PUBBLICITÀ COMPORTAMENTALE ONLINE

51. Spesso la pubblicità comportamentale online, nonché il tracciamento e la profilazione degli interessati che si accompagnano a tale forma di pubblicità, sono utilizzati per finanziare i servizi online. Il Gruppo di lavoro «Articolo 29» ha già espresso il proprio punto di vista su tale trattamento, dichiarando che:

    [la necessità contrattuale] non è un fondamento giuridico adeguato per creare un profilo dei gusti e delle scelte di stile di vita dell'utente sulla base della sequenza di clic che ha effettuato su un sito web e degli articoli che ha acquistato. Questo perché il [titolare] del trattamento dei dati non ha firmato un contratto per elaborare profili, bensì per fornire beni e servizi particolari, per esempio[28].

52. Di norma il trattamento di dati personali per finalità di pubblicità comportamentale non è necessario all'esecuzione di un contratto per servizi online. In via generale, sarebbe difficile sostenere che il contratto non è stato eseguito perché non vi erano annunci di pubblicità comportamentale. Ciò è tanto

più vero se si considera che gli interessati hanno il diritto assoluto, ai sensi dell'articolo 21, di opporsi al trattamento dei loro dati per finalità di marketing diretto.

53. Inoltre, l'articolo 6, paragrafo 1, lettera b), non può costituire un fondamento di liceità per la pubblicità comportamentale online per il solo fatto che tale pubblicità finanzia indirettamente la prestazione del servizio. Sebbene il trattamento in questione possa sostenere la prestazione di un servizio, ciò non è sufficiente di per sé per constatarne la necessità ai fini dell'esecuzione del contratto in essere. Il titolare del trattamento dovrebbe tenere conto dei fattori di cui al punto 33.

54. Considerando che la protezione dei dati è un diritto fondamentale garantito dall'articolo 8 della Carta dei diritti fondamentali, e che una delle finalità principali del RGPD è quella di fornire agli interessati il controllo sulle informazioni che li riguardano, i dati personali non possono essere considerati un bene commerciabile. Anche se l'interessato può acconsentire al trattamento di dati personali,[29] non può cedere i propri diritti fondamentali attraverso tale accordo[30].

55. Il comitato europeo per la protezione dei dati osserva altresì che, in linea con i requisiti in materia di tutela della vita privata nel settore delle comunicazioni elettroniche, con il parere del Gruppo di lavoro «Articolo 29» sulla pubblicità comportamentale[31] e con il documento di lavoro 02/2013 che fornisce orientamenti sull'ottenimento del consenso per i cookie[32], i titolari del trattamento devono ottenere il consenso preventivo degli interessati per installare i cookie necessari a svolgere attività di pubblicità comportamentale.

56. Il comitato europeo per la protezione dei dati rileva altresì che il monitoraggio e la profilazione degli utenti possono essere effettuati allo scopo di individuare gruppi di persone con caratteristiche simili, per consentire una pubblicità mirata a un pubblico di soggetti aventi caratteristiche simili. Tale trattamento non può essere svolto sulla base dell'articolo 6, paragrafo 1, lettera b), in quanto non si può affermare che tracciare e comparare le caratteristiche e i comportamenti dell'utente per finalità correlate alla pubblicità rivolta ad altre persone sia oggettivamente necessario all'esecuzione del contratto stipulato con l'utente[33].

3.4 TRATTAMENTO PER FINALITÀ DI PERSONALIZZAZIONE DEI CONTENUTI[34]

57. Il comitato europeo per la protezione dei dati riconosce che la personalizzazione del contenuto può costituire (ma non sempre costituisce) un elemento intrinseco e atteso di taluni servizi online e che pertanto in alcuni casi può essere considerata necessaria per l'esecuzione del contratto con l'utente di tali servizi. La possibilità che un siffatto trattamento possa essere considerato un elemento intrinseco di un servizio online dipenderà dalla natura del servizio prestato, dalle aspettative dell'interessato medio alla luce non soltanto delle condizioni del servizio, ma anche del modo in cui il servizio viene

promosso nei confronti degli utenti, e dalla possibilità di prestare il servizio anche in assenza di personalizzazione. Laddove la personalizzazione dei contenuti non sia oggettivamente necessaria ai fini del contratto sottostante, ad esempio se la fornitura di contenuti personalizzati è intesa a incrementare il coinvolgimento degli utenti in relazione a un servizio, ma non è parte integrante dell'utilizzo del servizio, i titolari del trattamento dovrebbero prendere in considerazione una base giuridica alternativa ove applicabile.

Esempio 7

Un motore di ricerca online di alberghi monitora le prenotazioni effettuate in passato dagli utenti al fine di creare un profilo delle rispettive spese abituali. Tale profilo viene successivamente utilizzato per raccomandare determinati alberghi all'utente nel presentare i risultati della ricerca. In questo caso la profilazione del comportamento pregresso e dei dati finanziari degli utenti non sarebbe oggettivamente necessaria all'esecuzione di un contratto, ossia la fornitura di servizi di ospitalità sulla base di particolari criteri di ricerca forniti dall'utente. Di conseguenza l'articolo 6, paragrafo 1, lettera b), non sarebbe applicabile a tale attività di trattamento.

Esempio 8

Un mercato online consente ai potenziali acquirenti di cercare e acquistare prodotti. Il mercato desidera mostrare suggerimenti personalizzati di prodotti sulla base dei contenuti precedentemente visualizzati dai potenziali acquirenti sulla piattaforma al fine di aumentare l'interattività. Questa personalizzazione non è oggettivamente necessaria per fornire il servizio offerto dal mercato. Di conseguenza un siffatto trattamento di dati personali non può fondarsi sull'articolo 6, paragrafo 1, lettera b), come base giuridica.

NOTE

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (RGPD).

[2] Cfr. anche considerando 44.

[3] Cfr. ad esempio la direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio e l'articolo 8 del RGPD.

[4] Cfr. considerando 18 della direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno.

[5] A tale proposito i titolari del trattamento devono rispettare gli obblighi di trasparenza stabiliti nel RGPD.

[6] Istituito a norma dell'articolo 68 del RGPD.

[7] Gruppo di lavoro «Articolo 29», Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva (CE) 95/46 (WP217). Cfr. in particolare le pagine 12, 13, 19, 20, 21, 22 e 65.

[8] Taluni dati personali dovrebbero rimanere privati o essere trattati esclusivamente secondo determinate modalità e il trattamento dei dati non dovrebbe risultare inatteso per l'interessato. Nel RGPD, il concetto di «ragionevoli aspettative» è specificamente menzionato nei considerando 47 e 50 in relazione all'articolo 6, paragrafo 1, lettera f) e all'articolo 6, paragrafo 4.

[9] Cfr. considerando 38 che fa riferimento al fatto che i minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali.

[10] Una clausola contrattuale che non è stata oggetto di negoziato individuale è abusiva ai sensi della direttiva sulle clausole abusive nei contratti «se, malgrado il requisito della buona fede, determina, a danno del consumatore, un significativo squilibrio dei diritti e degli obblighi delle parti derivanti dal contratto». Al pari dell'obbligo di trasparenza previsto dal RGPD, la direttiva sulle clausole abusive nei contratti impone l'uso di termini chiari e comprensibili. Di norma un trattamento di dati personali basato su quella che è considerata una clausola abusiva ai sensi della direttiva sulle clausole abusive nei contratti non sarà coerente con il requisito di cui all'articolo 5, paragrafo 1, lettera a), del RGPD secondo il quale il trattamento deve essere lecito e corretto.

[11] Il RGPD si applica a taluni titolari del trattamento al di fuori del SEE; cfr. l'articolo 3 di tale regolamento.

[12] Gruppo di lavoro «Articolo 29», *Working Party Opinion 03/2013 on purpose limitation* (Parere 03/2013 sulla limitazione delle finalità, WP203), pagg. 15 e 16 (versione inglese).

[13] Quando i titolari del trattamento si apprestano a individuare la base giuridica appropriata in linea con il principio di correttezza, troveranno difficile conseguire tale risultato se non hanno innanzitutto individuato chiaramente le finalità del trattamento oppure se il trattamento di dati personali va al di là di quanto necessario per le finalità specificate.

[14] Per maggiori informazioni sulle implicazioni in relazione all'articolo 9, cfr. Gruppo di lavoro «Articolo 29», «Linee guida sul consenso ai sensi del regolamento (UE) 2016/679 (WP259)», approvate dal comitato europeo per la protezione dei dati, pagg. 21 e 22.

[15] Gruppo di lavoro «Articolo 29», Linee guida sul consenso ai sensi del regolamento (UE) 2016/679 (WP259), approvate dal comitato europeo per la protezione dei dati, pag. 22.

[16] Nella sentenza *Huber* la Corte di giustizia dell'Unione europea ha affermato che «Si tratta quindi di una nozione autonoma [quella della necessità] del diritto comunitario che deve essere interpretata in maniera tale da rispondere pienamente alla finalità di tale direttiva [direttiva 95/46/CE] come definita dal suo art. 1, n. 1». Sentenza del 18 dicembre 2008, *Heinz Huber/Bundesrepublik Deutschland,* C-524/06, EU:C:2008:724, punto 52.

[17] Cfr. articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

[18] Cfr. strumentario del GEPD: Assessing the necessity of measures that limit the fundamental right to the protection of perso-

nal data (Valutazione della necessità di misure che limitano il diritto fondamentale alla protezione dei dati personali), pag. 5.

[19] Nella causa *Schecke*, la Corte ha stabilito che, nell'esaminare la necessità del trattamento di dati personali, il legislatore doveva tener conto di misure alternative, meno intrusive. Sentenza del 9 novembre 2010, *Volker und Markus Schecke GbR e Hartmut Eifert/Land Hessen*, cause riunite C-92/09 e C-93/09, EU:C:2010:662. Ciò è stato ribadito dalla Corte nella causa *Rīgas*, nella quale ha statuito che «[p]er quanto concerne la condizione relativa alla necessità del trattamento dei dati, si deve ricordare che le deroghe alla tutela dei dati personali e le limitazioni della stessa devono avvenire nei limiti dello stretto necessario». Sentenza del 4 maggio 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA «Rīgas satiksme»*, C-13/16, EU:C:2017:336, punto 30. Per imporre eventuali limitazioni all'esercizio del diritto alla tutela della vita privata e alla protezione dei dati personali in relazione al trattamento di dati personali occorre svolgere una verifica rigorosa di ciò che è «necessario»; cfr. strumentario del GEPD: *Assessing the necessity of measures that limit the fundamental right to the protection of personal data (Valutazione della necessità di misure che limitano il diritto fondamentale alla protezione dei dati personali)*, pag. 7.

[20] Gruppo di lavoro «Articolo 29», Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE (WP217), pag. 20.

[21] Ibidem, pag. 20.

[22] Cfr. Gruppo di lavoro «Articolo 29», Linee guida sul consenso ai sensi del regolamento (UE) 2016/679 (WP259), approvate dal comitato europeo per la protezione dei dati, pag. 35, nelle quali si afferma che: «[a]i sensi del regolamento [generale sulla protezione dei dati] non è possibile passare da una base giuridica a un'altra».

[23] Gruppo di lavoro «Articolo 29», Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE (WP217), pagg. 20 e 21.

[24] Ai sensi dell'articolo 5, paragrafo 1, lettera a), se un contratto viene successivamente invalidato, ciò avrà effetti sulla liceità del proseguimento del trattamento. Tuttavia ciò non implica automaticamente che la scelta dell'articolo 6, paragrafo 1, lettera b), come base giuridica, fosse errata.

[25] I servizi online possono altresì dover tenere conto della direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali (GU L 136 del 22.5.2019, pag. 1), che si applicherà a decorrere dal 1º gennaio 2022.

[26] Gruppo di lavoro «Articolo 29», Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE (WP217), pag. 20.

[27] Cfr. considerando 47, sesta frase.

[28] Gruppo di lavoro «Articolo 29», Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE (WP217), pag. 20.

[29] Cfr. direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.

[30] Oltre al fatto che l'uso dei dati personali è disciplinato dal RGPD, vi sono altri motivi per cui il trattamento dei dati personali si distingue concettualmente dai pagamenti monetari. Ad esempio, il denaro può essere contato, il che significa che è possibile confrontare i prezzi in un mercato concorrenziale e di norma i pagamenti in denaro possono essere effettuati soltanto con la partecipazione dell'interessato. Inoltre i dati personali possono essere sfruttati da più servizi contemporaneamente. Una volta perduto il controllo sui propri dati personali, non è detto che tale controllo possa essere ripristinato.

[31] Gruppo di lavoro «Articolo 29», Parere n. 2/2010 sulla pubblicità comportamentale online (WP171).

[32] Gruppo di lavoro «Articolo 29», *Working Document 02/2013 providing guidance on obtaining consent for cookies* (documento di lavoro 02/2013 sull'ottenimento del consenso per i cookie, WP208).

[33] Cfr. anche Gruppo di lavoro «Articolo 29», *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679* (WP251 rev.01), approvate dal comitato europeo per la protezione dei dati, pag. 14.

[34] I servizi online possono altresì dover tenere conto della direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali (GU L 136 del 22.5.2019, pag. 1), che si applicherà a decorrere dal 1º gennaio 2022.

Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video Versione 2.0

Adottate il 29 gennaio 2020

Cronologia delle versioni

Versione 2.0	29 gennaio 2020	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	10 luglio 2019	Adozione delle linee guida per la consultazione pubblica

Indice

1 Introduzione

2 Ambito di applicazione

- 2.1 Dati personali
- 2.2 Applicazione della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giudiziarie (direttiva LED)
- 2.3 Deroga relativa alle attività a carattere domestico

3 Liceità del trattamento

- 3.1 Legittimo interesse (articolo 6, paragrafo 1, lettera f))
  - 3.1.1 Esistenza di legittimi interessi
  - 3.1.2 Necessità del trattamento
  - 3.1.3 Bilanciamento degli interessi
- 3.2 Necessità allo scopo di eseguire un compito nell'interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (articolo 6, paragrafo 1, lettera e)).
- 3.3 Consenso (articolo 6, paragrafo 1, lettera a))

4 Comunicazione di filmati a terzi

- 4.1 Comunicazione di filmati a soggetti terzi in generale
- 4.2 Comunicazione di filmati alle autorità di contrasto

5 Trattamenti riguardanti categorie particolari di dati

- 5.1 Considerazioni generali sul trattamento dei dati biometrici
- 5.2 Misure proposte per ridurre al minimo i rischi durante il trattamento di dati biometrici

6 Diritti dell'interessato

- 6.1 Diritto di accesso
- 6.2 Diritto alla cancellazione e diritto di opposizione
  - 6.2.1 Diritto alla cancellazione (diritto all'oblio)
  - 6.2.2 Diritto di opposizione

7 Obblighi di trasparenza e informazione

- 7.1 Informazioni di primo livello (segnaletica di avvertimento)
  - 7.1.1 Posizionamento della segnaletica di avvertimento
  - 7.1.2 Contenuto delle informazioni di primo livello
- 7.2 Informazioni di secondo livello

8 Periodi di conservazione e obbligo di cancellazione

9 Misure tecniche e organizzative
9.1 Descrizione generale di un sistema di videosorveglianza
9.2 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita
9.3 Esempi concreti di misure pertinenti
9.3.1 Misure organizzative
9.3.2 Misure tecniche

10 Valutazione d'impatto sulla protezione dei dati

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

Considerando l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE («RGPD»),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo n. 37 dello stesso, modificati dalla decisione n. 154/2018 del Comitato misto SEE del 6 luglio 2018[1],

visti l'articolo 12 e l'articolo 22 del regolamento interno,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

1. INTRODUZIONE

1. L'uso intensivo di dispositivi video influisce sul comportamento dei cittadini. Un ricorso significativo a tali strumenti in numerosi ambiti della vita delle persone eserciterà su queste ultime un'ulteriore pressione per impedire il rilevamento di quelle che potrebbero essere percepite come anomalie. Di fatto, queste tecnologie possono limitare le possibilità di muoversi e di utilizzare servizi in maniera anonima nonché, in linea generale, la possibilità di passare inosservati. Le conseguenze per la protezione dei dati sono enormi.
2. Mentre le persone potrebbero essere a proprio agio con la videosorveglianza installata, ad esempio, per una determinata finalità di sicurezza, occorre assicurare che non ne venga fatto un uso improprio per scopi totalmente diversi e inaspettati per l'interessato (ad esempio, per scopi di marketing, controllo delle prestazioni dei dipendenti, ecc.). Inoltre, attualmente si utilizzano molti strumenti per sfruttare le immagini acquisite e trasformare le telecamere tradizionali in telecamere intelligenti. La quantità di dati generati da video, unitamente a questi strumenti e tecniche, aumenta i rischi di un uso secondario (correlato o meno allo scopo al quale viene inizialmente destinato il sistema) o persino improprio. Nel gestire la videosorveglianza sarebbe opportuno considerare sempre attentamente i principi generali del RGPD (articolo 5).
3. I sistemi di videosorveglianza incidono in svariati modi sulle interazioni messe in atto dai professionisti del settore privato e pubblico in luoghi pubblici o privati allo scopo di migliorare la sicurezza, analizzare le risposte del pubblico, fornire pubblicità personalizzata, ecc. La videosorveglianza è diventata un sistema ad alte prestazioni grazie alla crescente applicazione di analisi video intelligenti. Queste tecniche possono essere più intrusive (tecnologie biometriche complesse) o meno intrusive (semplici algoritmi di conteggio). Restare anonimi e preservare la propria privacy è, in linea generale, sempre più difficile. Le questioni relative alla protezione dei dati sollevate nelle diverse situazioni possono essere diverse, così come l'analisi giuridica riferita all'utilizzo dell'una o dell'altra di queste tecnologie.
4. Oltre alle questioni di privacy, sussistono anche i rischi legati a possibili malfunzionamenti di questi dispositivi e alle distorsioni che possono indurre. I ricercatori riferiscono che il software utilizzato per l'identificazione, il riconoscimento o l'analisi facciale funziona in modo diverso in base all'età, al genere e all'etnia della persona che sta identificando. Le prestazioni degli algoritmi sembrano variare in rapporto ai dati demografici, per cui una distorsione nel riconoscimento facciale minaccia di rafforzare il pregiudizio sociale. Per questo motivo, i titolari del trattamento devono anche assicurare che il trattamento dei dati biometrici derivanti dalla videosorveglianza sia soggetto a una valutazione periodica della sua pertinenza e dell'adeguatezza delle garanzie fornite.
5. La videosorveglianza non è di per sé indispensabile se esistono altri mezzi per raggiungere lo scopo che ci si prefigge. Altrimenti si rischia di modificare le norme culturali con la conseguenza di ammettere come regola l'assenza di privacy .

6. Le presenti linee guida mirano a fornire indicazioni sull'applicazione del RGPD in relazione al trattamento di dati personali attraverso dispositivi video. Gli esempi non sono esaustivi e il ragionamento generale può essere applicato a tutte le potenziali aree di utilizzo.

2. AMBITO DI APPLICAZIONE[2]

2.1 DATI PERSONALI

7. La sorveglianza sistematica e automatizzata di uno spazio specifico con mezzi ottici o audiovisivi, per lo più a scopo di protezione della proprietà, o per proteggere la vita e la salute delle persone, è divenuta un fenomeno significativo dei nostri giorni. Questa attività comporta la raccolta e la conservazione di informazioni grafiche o audiovisive su tutte le persone che entrano nello spazio monitorato, identificabili in base al loro aspetto o ad altri elementi specifici. L'identità di tali persone può essere stabilita sulla base delle informazioni così raccolte. Questo tipo di sorveglianza consente inoltre un ulteriore trattamento dei dati personali per quanto riguarda la presenza e il comportamento delle persone nello spazio considerato. Il rischio potenziale di un uso improprio di tali dati aumenta in rapporto alla dimensione dello spazio monitorato e al numero di persone che lo frequentano. Ciò si riflette nel RGPD all'articolo 35, paragrafo 3, lettera c), che impone l'esecuzione di una valutazione d'impatto sulla protezione dei dati in caso di sorveglianza sistematica su vasta scala di un'area accessibile al pubblico, e all'articolo 37, paragrafo 1, lettera b), che impone ai responsabili del trattamento di designare un responsabile della protezione dei dati se la tipologia di trattamento, per sua natura, richiede il monitoraggio regolare e sistematico degli interessati.
8. Tuttavia, il regolamento non si applica al trattamento di dati che non hanno alcun riferimento a una persona, ad esempio se una persona non può essere identificata, direttamente o indirettamente.

9. Esempio Il RGPD non è applicabile alle fotocamere false (vale a dire qualsiasi fotocamera che non funziona come una fotocamera e quindi non elabora alcun dato personale). Tuttavia, in alcuni Stati membri potrebbero essere applicabili altre normative.

   Esempio Le registrazioni ad alta quota rientrano nell'ambito di applicazione del RGPD solo se, in queste circostanze, i dati trattati possono essere correlati a una determinata persona.

   Esempio Una videocamera è integrata in un'automobile per fornire assistenza al parcheggio. Se la videocamera è costruita o regolata in modo tale da non raccogliere alcuna informazione relativa a una persona fisica (ad esempio targhe o informazioni che potrebbero identificare i passanti), il RGPD non è applicabile.

2.2 APPLICAZIONE DELLA DIRETTIVA (UE) 2016/680 SULLA PROTEZIONE DEI DATI NELLE ATTIVITÀ DI POLIZIA E GIUDIZIARIE (DIRETTIVA LED)

10. Il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, rientra nella direttiva (UE) 2016/680.

2.3 DEROGA RELATIVA ALLE ATTIVITÀ A CARATTERE DOMESTICO

11. Ai sensi dell'articolo 2, paragrafo 2, lettera c), il trattamento di dati personali da parte di una persona fisica nel corso di un'attività a carattere esclusivamente personale o domestico, che può anche includere attività online, esula dall'ambito di applicazione del RGPD[3].

12. Questa disposizione – la cosiddetta deroga relativa alle attività a carattere domestico – nel contesto della videosorveglianza deve essere interpretata in modo restrittivo. Di conseguenza, come ritenuto dalla Corte di giustizia dell'Unione europea, la cosiddetta «deroga relativa alle attività a carattere domestico» deve *«[...] interpretarsi nel senso che comprende unicamente le attività che rientrano nell'ambito della vita privata o familiare dei singoli, il che manifestamente non avviene nel caso del trattamento di dati personali consistente nella loro pubblicazione su Internet in modo da rendere tali dati accessibili ad un numero indefinito di persone»*[4]*. Inoltre, un sistema di videosorveglianza, nella misura in cui comporta la registrazione e la conservazione costanti di dati personali e si estende «anche se solo parzialmente, allo spazio pubblico, e pertanto è dirett[o] verso l'esterno della sfera privata della persona che procede al trattamento dei dati con tale modalità, [...] non può essere considerat[o] un'attività esclusivamente "personale o domestica" ai sensi dell'articolo 3, paragrafo 2, secondo trattino, della direttiva 95/46»*[5].

13. I dispositivi video azionati all'interno dei locali di un privato possono rientrare nella deroga relativa alle attività a carattere domestico. Ciò dipenderà da diversi fattori, che dovranno essere presi in considerazione nella loro totalità per giungere a una conclusione. Oltre agli elementi summenzionati individuati dalle sentenze della Corte di giustizia dell'Unione europea, chi utilizza la videosorveglianza presso il proprio domicilio deve verificare se ha un qualche tipo di rapporto personale con l'interessato, se la portata o la frequenza della sorveglianza siano indicative di una qualche forma di attività professionale da parte sua e il potenziale impatto negativo della sorveglianza sugli interessati. La presenza di uno qualsiasi degli elementi summenzionati non implica necessariamente che il trattamento non rientri nell'ambito di applicazione della deroga relativa alle attività a carattere domestico; per stabilirlo è infatti necessaria una valutazione complessiva.

14. Esempio Per documentare le sue vacanze, un turista registra video sia con il suo cellulare sia con una videocamera. Mostra il filmato ad amici e familiari, ma non lo rende accessibile a un numero indefinito

di persone. Questo caso rientrerebbe nella deroga relativa alle attività a carattere domestico.

Esempio Una ciclista in mountain bike vuole registrare il suo percorso in discesa con una telecamera sportiva. Attraversa una zona isolata e prevede di utilizzare le registrazioni solo per intrattenimento personale e nel suo domicilio. Questo caso rientrerebbe nella deroga relativa alle attività a carattere domestico anche se vi fosse in una certa misura un trattamento di dati personali.

Esempio: Qualcuno sorveglia e registra il proprio giardino. La proprietà è recintata e soltanto il titolare del trattamento e la sua famiglia entrano regolarmente in giardino. Questo caso rientrerebbe nella deroga relativa alle attività a carattere domestico, a condizione che la videosorveglianza non si estenda, neppure parzialmente, a uno spazio pubblico o a una proprietà confinanti.

3. LICEITÀ DEL TRATTAMENTO

15. Prima di procedere, si devono specificare dettagliatamente le finalità del trattamento (articolo 5, paragrafo 1, lettera b)). La videosorveglianza può servire a molti scopi, ad esempio a supporto della protezione della proprietà e di altri beni, della protezione della vita e dell'integrità fisica delle persone o a raccogliere elementi di prova in vista di procedimenti giudiziari civili[6]. Queste finalità del monitoraggio devono essere documentate per iscritto (articolo 5, paragrafo 2) e devono essere specificate per ogni telecamera di sorveglianza in uso. Le telecamere utilizzate per lo stesso scopo da un unico titolare del trattamento possono essere oggetto di una documentazione unitaria. Inoltre, gli interessati devono essere informati delle finalità del trattamento ai sensi dell'articolo 13 (*si veda la sezione 7, Obblighi di trasparenza e di informazione*). La semplice menzione di uno scopo di «sicurezza» o «per la vostra sicurezza» con riguardo alla videosorveglianza non è sufficientemente specifica (articolo 5, paragrafo 1, lettera b)). Ciò contrasta inoltre con il principio secondo il quale i dati personali vengono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato [cfr. articolo 5, paragrafo 1, lettera a)].

16. In linea di principio, ogni fondamento di diritto ai sensi dell'articolo 6, paragrafo 1, può fornire una base giuridica per il trattamento dei dati di videosorveglianza. Ad esempio, l'articolo 6, paragrafo 1, lettera c), si applica quando la normativa nazionale prevede l'obbligo di mettere in atto in sistema di videosorveglianza[7]. Tuttavia, nella pratica, le disposizioni più suscettibili di essere utilizzate sono

- Articolo 6, paragrafo 1, lettera f) (legittimo interesse)
- Articolo 6, paragrafo 1, lettera e) (necessità al fine di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri).

In casi piuttosto eccezionali il titolare del trattamento potrebbe invocare l'ar-

ticolo 6, paragrafo 1, lettera a) (consenso) come base giuridica .

3.1 LEGITTIMO INTERESSE (ARTICOLO 6, PARAGRAFO 1, LETTERA F))

17. L'analisi giuridica della disposizione contenuta all'articolo 6, paragrafo 1, lettera f), dovrebbe basarsi sui criteri indicati di seguito, conformemente al considerando 47.

3.1.1 ESISTENZA DI LEGITTIMI INTERESSI

18. La videosorveglianza è lecita se è necessaria per conseguire la finalità di un legittimo interesse perseguito da un titolare del trattamento o da un terzo, a meno che su tali interessi prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato (articolo 6, paragrafo 1, lettera f)). I legittimi interessi perseguiti da un titolare del trattamento o da terzi possono avere natura giuridica[8], economica o immateriale[9]. Tuttavia, il titolare del trattamento dovrebbe considerare che se l'interessato si oppone alla sorveglianza a norma dell'articolo 21, si può procedere alla videosorveglianza di tale interessato soltanto se il legittimo interesse in questione ha natura cogente e prevale sugli interessi, i diritti e le libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

19. In presenza di una situazione di reale rischio, la tutela della proprietà da furti o atti vandalici può costituire un legittimo interesse con riguardo alla videosorveglianza.

20. Il legittimo interesse deve essere esistente e attuale (ossia non deve essere fittizio o ipotetico)[10]. Prima di avviare la sorveglianza è necessario che sussista una situazione di reale difficoltà, come ad esempio danni o incidenti gravi verificatisi in passato. Alla luce del principio di responsabilizzazione, i titolari del trattamento farebbero bene a documentare gli eventi problematici in questione (data, modalità, perdita finanziaria) e le relative accuse penali. Tali casi documentati possono costituire un solido elemento di prova per l'esistenza di un legittimo interesse. L'esistenza di un legittimo interesse e la necessità del monitoraggio dovrebbero essere oggetto di riesame periodico (ad esempio, una volta all'anno, a seconda delle circostanze).

21. Esempio Un negoziante vuole aprire un nuovo esercizio commerciale e installare un sistema di videosorveglianza per prevenire atti vandalici. Può dimostrare, presentando delle statistiche, che nel quartiere è alta la probabilità di eventi vandalici . E' utile anche l'esperienza degli esercizi commerciali posti in prossimità. Non è necessario che il titolare del trattamento in questione abbia subito un danno. Nella misura in cui dai danni subiti nel quartiere emerga una situazione di pericolo o comunque analoga, può esservi un'indicazione dell'esistenza di un legittimo interesse. Tuttavia, non è sufficiente presentare statistiche

nazionali o generali sulla criminalità senza analizzare l'area in questione o i pericoli per lo specifico esercizio commerciale.

22. Le situazioni di pericolo imminente possono configurare un legittimo interesse, per esempio nel caso di banche o negozi che vendono beni preziosi (ad esempio, gioiellerie) o di luoghi che sono notoriamente teatro di reati contro il patrimonio (ad esempio, stazioni di servizio).
23. Il RGPD stabilisce inoltre chiaramente che le autorità pubbliche non possono invocare il legittimo interesse per i trattamenti svolti nell'esecuzione dei loro compiti. Cfr. articolo 6, paragrafo 1, seconda frase.

3.1.2 NECESSITÀ DEL TRATTAMENTO

24. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»). Cfr. articolo 5, paragrafo 1, lettera c). Prima di installare un sistema di videosorveglianza, il titolare del trattamento deve sempre valutare criticamente se questa misura sia in primo luogo idonea a raggiungere l'obiettivo desiderato e, in secondo luogo, adeguata e necessaria per i suoi scopi. Si dovrebbe optare per misure di videosorveglianza unicamente se la finalità del trattamento non può ragionevolmente essere raggiunta con altri mezzi meno intrusivi per i diritti e le libertà fondamentali dell'interessato.
25. In una situazione in cui un titolare del trattamento intenda prevenire reati legati al patrimonio, invece di installare un sistema di videosorveglianza potrebbe adottare misure di sicurezza alternative, come la recinzione della proprietà, il pattugliamento regolare di personale di sicurezza, l'impiego di custodi, una migliore illuminazione, l'installazione di serrature di sicurezza, finestre e porte a prova di manomissione o l'applicazione di rivestimento anti-graffiti o lamine alle pareti. Tali misure possono essere efficaci quanto i sistemi di videosorveglianza contro furti e vandalismi. Il titolare del trattamento deve valutare caso per caso se tali misure possano essere una soluzione ragionevole.
26. Prima di utilizzare un sistema di telecamere, il titolare del trattamento è tenuto a valutare dove e quando siano assolutamente necessarie misure di videosorveglianza. Di solito un sistema di sorveglianza funzionante sia di notte sia al di fuori del normale orario di lavoro soddisfa le esigenze del titolare del trattamento di prevenire pericoli per il suo patrimonio.
27. In generale, la necessità di utilizzare la videosorveglianza per proteggere la proprietà di un titolare si arresta ai confini della proprietà stessa[11]. Tuttavia, vi sono casi in cui la sorveglianza della proprietà non è sufficiente per una protezione efficace. In alcuni singoli casi potrebbe essere necessario estendere la videosorveglianza alle immediate vicinanze dell'area di proprietà. In tale contesto, il titolare del trattamento dovrebbe prendere in considerazio-

ne l'impiego di mezzi fisici e tecnici, ad esempio bloccando o oscurando le zone non pertinenti.

28. Esempio Una libreria vuole proteggere la propria sede contro atti di vandalismo. In linea generale, le telecamere dovrebbero riprendere soltanto i locali in senso stretto; non è infatti necessario sorvegliare i locali adiacenti o le zone pubbliche circostanti la sede della libreria per tale scopo.

29. Occorre interrogarsi sulla necessità del trattamento anche per quanto riguarda le modalità di conservazione di elementi di prova . In alcuni casi potrebbe essere necessario utilizzare soluzioni tipo scatola nera, nelle quali il filmato viene automaticamente cancellato dopo un determinato periodo di conservazione e vi si accede solo in caso di eventi problematici. In altre situazioni potrebbe non essere affatto necessario registrare il materiale video, essendo magari più opportuno ricorrere al monitoraggio in tempo reale. La scelta tra le due soluzioni dovrebbe anche basarsi sullo scopo perseguito. Se, ad esempio, la videosorveglianza è finalizzata alla raccolta di prove, solitamente i metodi in tempo reale non sono adatti. Talvolta il monitoraggio in tempo reale può risultare anche più intrusivo rispetto alla conservazione e alla cancellazione automatica delle registrazioni dopo un lasso di tempo limitato (ad esempio, se un operatore visualizza costantemente le immagini su monitor, questo metodo potrebbe essere più intrusivo rispetto alla conservazione diretta del materiale in una scatola nera in assenza di monitoraggio). In questo contesto occorre avere riguardo al principio della minimizzazione dei dati (articolo 5, paragrafo 1, lettera c)). Occorre inoltre tenere presente la possibilità per il titolare del trattamento di avvalersi di personale di sicurezza in grado di reagire e intervenire immediatamente anziché ricorrere alla videosorveglianza.

3.1.3 BILANCIAMENTO DEGLI INTERESSI

30. Supponendo che la videosorveglianza sia necessaria per proteggere i legittimi interessi di un titolare del trattamento, un sistema di videosorveglianza può essere messo in funzione unicamente se sui legittimi interessi del titolare del trattamento o su quelli di terzi (ad esempio, la protezione della proprietà o dell'integrità fisica) non prevalgono gli interessi o i diritti e le libertà fondamentali dell'interessato. Il titolare del trattamento deve valutare 1) in che misura il monitoraggio incida sugli interessi, sui diritti fondamentali e sulle libertà degli individui, e 2) se ciò comporti violazioni o conseguenze negative rispetto ai diritti dell'interessato. Di fatto, il bilanciamento degli interessi è d'obbligo. I diritti e le libertà fondamentali, da un lato, e i legittimi interessi del titolare del trattamento, dall'altro, vanno valutati e bilanciati con attenzione.

31. Esempio Una libreria vuole proteggere la propria sede contro atti di vandalismo. In linea generale, le telecamere dovrebbero riprendere soltanto i locali in senso stretto; non è infatti necessario sorvegliare i locali adiacenti o le zone pubbliche circostanti la sede della libreria per tale scopo.

3.1.3.1 Decidere caso per caso

32. Poiché il bilanciamento degli interessi è obbligatorio ai sensi del regolamento, la decisione deve essere presa caso per caso (cfr. articolo 6, paragrafo 1, lettera f)). Non è sufficiente fare riferimento a situazioni astratte o confrontare casi simili tra loro. Il titolare del trattamento deve valutare i rischi di interferenza nei diritti dell'interessato; in questo caso il criterio decisivo è l'intensità dell'intervento rispetto ai diritti e allele libertà dell'individuo.

33. L'intensità può essere definita, tra l'altro, dal tipo di informazioni raccolte (contenuto delle informazioni), dalla portata (densità delle informazioni, estensione territoriale e geografica), dal numero di interessati coinvolti – come numero specifico o come percentuale della popolazione interessata – dalla situazione specifica, dagli interessi effettivi del gruppo di interessati, dalla disponibilità di strumenti mezzi alternativi nonché dalla natura e dalla portata della valutazione dei dati.

34. Importanti fattori di bilanciamento possono essere le dimensioni della zona e il numero di interessati sotto sorveglianza. L'uso della videosorveglianza in una zona isolata (ad esempio, per osservare la fauna selvatica o per proteggere infrastrutture critiche come un'antenna radio privata) deve essere valutato in modo diverso rispetto alla videosorveglianza in una zona pedonale o in un centro commerciale.

35. Esempio Se è installata una telecamera da cruscotto (dash cam) – ad esempio, allo scopo di raccogliere prove in caso di incidente – è importante assicurarsi che la telecamera non registri costantemente il traffico, così come le persone che si trovano vicino a una strada. In caso contrario, l'interesse ad avere le videoregistrazioni come elemento di prova nel caso ipotetico di un incidente stradale non può giustificare questa grave interferenza nei diritti degli interessati

3.1.3.2 Ragionevoli aspettative degli interessati

36. Secondo il considerando 47, l'esistenza di un legittimo interesse richiede un'attenta valutazione. A questo proposito, occorre includere le ragionevoli aspettative dell'interessato al momento e nel contesto del trattamento dei suoi dati personali. Per quanto riguarda la sorveglianza sistematica, il rapporto tra l'interessato e il titolare del trattamento può variare significa-

tivamente e può influenzare le ragionevoli aspettative dell'interessato. L'interpretazione del concetto di aspettativa ragionevole non dovrebbe basarsi soltanto sulle aspettative soggettive in questione. Il criterio decisivo deve essere invece se un soggetto terzo imparziale possa ragionevolmente aspettarsi e concludere di essere oggetto di sorveglianza nella situazione specifica.

37. Ad esempio, nella maggior parte dei casi un dipendente sul luogo di lavoro non si aspetta di essere monitorato dal proprio datore di lavoro[12]. Inoltre, non ci si aspetta sorveglianza nel proprio giardino, in locali abitati o in ambulatori e sale di terapia. Analogamente, non è ragionevole aspettarsi sorveglianza nei servizi sanitari o nelle saune; la sorveglianza in questo tipo di zone costituisce una grave interferenza nei diritti dell'interessato. Le ragionevoli aspettative degli interessati sono quindi che non si attui alcuna videosorveglianza in tali zone. D'altro canto, il cliente di una banca potrebbe aspettarsi di essere sorvegliato all'interno della banca o presso un bancomat.

38. Gli interessati possono anche aspettarsi di non essere sorvegliati all'interno di aree accessibili al pubblico – soprattutto se tali aree sono solitamente utilizzate per la convalescenza, la rigenerazione e per attività ricreative – nonché nei luoghi in cui le persone trascorrono del tempo e/o interagiscono, come ad esempio zone di seduta, tavoli in ristoranti, parchi, cinema e strutture per il fitness. In questo caso gli interessi o i diritti e le libertà dell'interessato spesso prevarranno sui legittimi interessi del titolare del trattamento.

39. Esempio Nei servizi igienici gli interessati si aspettano di non essere sorvegliati. La videosorveglianza, ad esempio, per prevenire incidenti non è uno strumento proporzionato

40. La presenza di segnaletica che informa l'interessato in merito alla videosorveglianza è del tutto irrilevante al fine di determinare ciò che un interessato può oggettivamente aspettarsi. Ciò significa, ad esempio, che il proprietario di un esercizio commerciale non può fare affidamento sull'esistenza oggettiva di una ragionevole aspettativa da parte dei clienti riguardo al monitoraggio solo perché un cartello all'ingresso li informa della presenza di un sistema di sorveglianza.

3.2 NECESSITÀ ALLO SCOPO DI ESEGUIRE UN COMPITO NELL'INTERESSE PUBBLICO O CONNESSO ALL'ESERCIZIO DI PUBBLICI POTERI DI CUI È INVESTITO IL TITOLARE DEL TRATTAMENTO (ARTICOLO 6, PARAGRAFO 1, LETTERA E)).

41. I dati personali potrebbero essere trattati mediante la videosorveglianza a norma dell'articolo 6, paragrafo 1, lettera e), se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri[13]. Può darsi che l'esercizio di pubblici poteri non consenta tale trattamento, ma altri fondamenti di liceità, per esempio obiettivi di «salute e sicurezza» per la protezione di visitatori e dipendenti, possono fornire

un margine limitato per il trattamento, in ogni caso tenendo conto degli obblighi previsti dal RGPD e dei diritti degli interessati.

42. Gli Stati membri possono mantenere o introdurre una normativa nazionale specifica in materia di videosorveglianza per adattare l'applicazione delle norme del RGPD, determinando con maggiore precisione specifici requisiti per il trattamento, purché siano conformi ai principi stabiliti dal RGPD (ad esempio, limitazione della conservazione, proporzionalità).

3.3 CONSENSO (ARTICOLO 6, PARAGRAFO 1, LETTERA A))

43. Il consenso deve essere prestato liberamente, deve essere specifico, informato e inequivocabile, come descritto nelle linee guida sul consenso[14].

44. Per quanto riguarda la sorveglianza sistematica, il consenso dell'interessato può fungere da base giuridica ai sensi dell'articolo 7 (cfr. il considerando 43) solo in casi eccezionali. È nella natura della sorveglianza il fatto che questa tecnologia consenta di controllare contemporaneamente un numero non noto di persone. Il titolare del trattamento difficilmente sarà in grado di dimostrare che l'interessato ha prestato il consenso prima del trattamento dei suoi dati personali (articolo 7, paragrafo 1). Supponendo che l'interessato revochi il proprio consenso, sarà difficile per il titolare dimostrare che i dati personali non sono più oggetto di trattamento (articolo 7, paragrafo 3).

45. Esempio Gli atleti possono chiedere di essere monitorati durante gli esercizi individuali al fine di analizzare tecniche e prestazioni. D'altra parte, quando una società sportiva prende l'iniziativa di monitorare un'intera squadra per la stessa finalità, il consenso spesso non sarà valido, in quanto i singoli atleti possono sentirsi costretti a prestare il proprio consenso per evitare che un loro eventuale rifiuto si ripercuota negativamente sui compagni di squadra.

46. Se il titolare del trattamento desidera invocare il consenso, è suo dovere assicurarsi che ogni interessato che entra nella zona sottoposta a videosorveglianza abbia prestato il proprio consenso. Tale consenso deve soddisfare le condizioni di cui all'articolo 7. L'ingresso in una zona sorvegliata contrassegnata (ad esempio, le persone sono invitate a passare attraverso uno specifico corridoio o cancello per accedere a una zona sorvegliata), non configura una dichiarazione o una chiara azione affermativa come necessarie per la validità del consenso, a meno che siano soddisfatti i criteri di cui agli articoli 4 e 7 descritti nelle linee guida sul consenso[15].

47. Dato lo squilibrio di potere tra datori di lavoro e dipendenti, nella maggior parte dei casi i datori di lavoro non dovrebbero invocare il consenso nel trattare i dati personali, in quanto è improbabile che quest'ultimo venga fornito liberamente. In tale contesto si dovrebbe tener conto delle linee guida sul consenso.

48. La legge degli Stati membri o i contratti collettivi, compresi i «contratti di lavoro», possono prevedere norme specifiche sul trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro (cfr. l'articolo 88).

4. COMUNICAZIONE DI FILMATI A TERZI

49. In linea di principio, le norme generali del RGPD si applicano alla comunicazione di videoregistrazioni a soggetti terzi.

4.1 COMUNICAZIONE DI FILMATI A SOGGETTI TERZI IN GENERALE

50. La comunicazione è definita all'articolo 4, paragrafo 2, come trasmissione (comunicazione individuale), diffusione (pubblicazione online) o qualsiasi altra forma di messa a disposizione. I soggetti terzi sono definiti all'articolo 4, paragrafo 10. In caso di comunicazione a paesi terzi o organizzazioni internazionali, si applicano anche le disposizioni speciali dall'articolo 44 e seguenti.

51. Qualsiasi comunicazione di dati personali costituisce uno specifico trattamento per il quale il titolare deve avere una base giuridica fra quelle di cui all'articolo 6.

52. Esempio Il titolare del trattamento che desidera caricare una registrazione su Internet deve fare riferimento a una base giuridica per tale trattamento, ad esempio ottenendo il consenso dell'interessato ai sensi dell'articolo 6, paragrafo 1, lettera a).

53. La trasmissione di filmati a terzi per scopi diversi da quelli per i quali i dati sono stati raccolti è possibile a norma dell'articolo 6, paragrafo 4.

54. Esempio La barriera di un parcheggio è videosorvegliata allo scopo di risolvere le cause per danni. Quando si verifica un danno, la registrazione viene ceduta a un avvocato per la trattazione di una causa. In questo caso lo scopo della registrazione coincide con quello della trasmissione.

Esempio La barriera di un parcheggio è videosorvegliata allo scopo di risolvere le cause per danni. La registrazione viene pubblicata online per puro divertimento. In questo caso lo scopo è diverso e non è compatibile con lo scopo iniziale. Sarebbe inoltre problematico individuare una base giuridica per tale trattamento (pubblicazione).

55. Il terzo destinatario dovrà effettuare una propria analisi giuridica, in particolare individuando la base giuridica del suo trattamento (per esempio, la ricezione dei materiali filmati) ai sensi dell'articolo 6 .

4.2 COMUNICAZIONE DI FILMATI ALLE AUTORITÀ DI CONTRASTO

56. Anche la comunicazione di videoregistrazioni alle autorità di contrasto è un processo indipendente, per il quale il titolare del trattamento deve individuare una separata giustificazione.

57. Secondo l'articolo 6, paragrafo 1, lettera c), il trattamento è lecito se è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento. Sebbene le attività di polizia siano disciplinate in via esclusiva dalle norme vigenti nei singoli Stati membri, è molto probabile che esistano norme generali che disciplinano il trasferimento delle prove alle autorità di contrasto in ogni Stato membro. Il trattamento eseguito dal titolare che consegna i dati è disciplinato dal RGPD. Se la normativa nazionale impone al titolare del trattamento di cooperare con le autorità di contrasto (per esempio nelle indagini), la base giuridica per la trasmissione dei dati è un obbligo legale di cui all'articolo 6, paragrafo 1, lettera c).

58. Spesso, quindi, il rispetto dei requisiti di limitazione della finalità di cui all'articolo 6, paragrafo 4, non risulta problematico, in quanto la comunicazione è disciplinata esplicitamente dal diritto degli Stati membri. Non è quindi necessario prendere in considerazione i requisiti specifici riferiti all'eventuale cambiamento di finalità ai sensi delle lettere a)-e) dell'Articolo 6, paragrafo 4.

59. Esempio Il proprietario di un esercizio commerciale registra i filmati dell'impianto di videosorveglianza posto all'ingresso dello stesso. Un filmato mostra una persona che ruba il portafoglio di un'altra persona. La polizia chiede al titolare del trattamento di consegnare il materiale per assisterla nelle indagini. In questo caso, il proprietario dell'esercizio commerciale utilizzerebbe la base giuridica di cui all'articolo 6, paragrafo 1, lettera c) (obbligo legale), in combinato disposto con la normativa nazionale applicabile per il trattamento consistente nella comunicazione dei materiali.

60. Esempio Una telecamera viene installata in un esercizio commerciale per motivi di sicurezza. Il proprietario crede di aver registrato qualcosa di sospetto e decide di inviare il materiale alla polizia (senza alcuna indicazione che vi sia un'indagine in corso). In questo caso il proprietario dell'esercizio commerciale deve valutare se sono soddisfatte le condizioni previste, nella maggior parte dei casi, dall'articolo 6, paragrafo 1, lettera f) – come per esempio qualora abbia un ragionevole sospetto che sia stato commesso un reato.

61. Il trattamento dei dati personali da parte delle autorità di contrasto non è disciplinato dal RGPD (si veda l'articolo 2, paragrafo 2, lettera d)), bensì dalla direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giudiziarie.

5. TRATTAMENTI RIGUARDANTI CATEGORIE PARTICOLARI DI DATI

62. Solitamente, i sistemi di videosorveglianza raccolgono enormi quantità di dati personali che possono rivelare dati di natura altamente personale e persino categorie particolari di dati. Infatti, dati apparentemente non significativi, all'origine raccolti tramite video, possono essere utilizzati per ricavare altre informazioni e raggiungere uno scopo diverso da quello iniziale (ad esempio per mappare le abitudini di un individuo). Tuttavia, la videosorveglianza non sempre è considerata un trattamento di categorie particolari di dati personali.

63. Esempio Le riprese video che mostrano un interessato che indossa occhiali o utilizza una sedia a rotelle non sono di per sé considerate categorie particolari di dati personali.

64. Tuttavia, se le riprese video sono trattate per ricavare categorie particolari di dati, si applica l'articolo 9.

65. Esempio Si potrebbero, ad esempio, dedurre le opinioni politiche da immagini che mostrano interessati identificabili mentre partecipano a un evento, a uno sciopero, ecc. Questo caso rientrerebbe nell'ambito di applicazione dell'articolo 9.

    Esempio Un ospedale che installa una videocamera per monitorare le condizioni di salute di un paziente effettua un trattamento di categorie particolari di dati personali (articolo 9).

66. In via generale e in linea di principio, ogniqualvolta si installa un sistema di videosorveglianza si dovrebbe prestare particolare attenzione al principio della minimizzazione dei dati. Pertanto, anche nei casi in cui l'articolo 9, paragrafo 1, non si applica, il titolare del trattamento dovrebbe sempre cercare di ridurre al minimo il rischio di acquisire filmati che rivelino altri dati sensibili (al di là dell'articolo 9), indipendentemente dalla finalità.

67. Esempio Un'attività di videosorveglianza che acquisisce le immagini di una chiesa non rientra di per sé nel campo di applicazione dell'articolo 9. Tuttavia, il titolare del trattamento deve effettuare una valutazione particolarmente attenta ai sensi dell'articolo 6, paragrafo 1, lettera f), con riguardo agli interessi della persona interessata, tenendo conto della natura dei dati nonché del rischio di acquisire altri dati sensibili (ulteriori rispetto a quelli di cui all'articolo 9) .

68. Se un sistema di videosorveglianza è utilizzato per trattare categorie particolari di dati, il titolare del trattamento deve individuare sia un'eccezione che

consenta il trattamento di categorie particolari di dati ai sensi dell'articolo 9 (vale a dire un'esenzione dal divieto generale di trattare categorie particolari di dati) sia una base giuridica ai sensi dell'articolo 6.

69. Ad esempio, si potrebbe utilizzare l'articolo 9, paragrafo 2, lettera c) *«[...] il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica [...]»)* – in teoria e in via del tutto eccezionale – ma il titolare del trattamento dovrebbe giustificarlo come una necessità assoluta per tutelare gli interessi vitali di tale persona e dimostrare che «[...] l'interessato *si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso»*. Inoltre, il titolare del trattamento non potrà utilizzare il sistema per nessun altro motivo.
70. È importante rilevare in questa sede che probabilmente non tutte le esenzioni elencate all'articolo 9 sono utilizzabili per giustificare il trattamento di categorie particolari di dati attraverso la videosorveglianza. Più specificamente, i titolari che trattano tali dati nell'ambito della videosorveglianza non possono invocare l'articolo 9, paragrafo 2, lettera e), che consente il trattamento di dati personali resi manifestamente pubblici dall'interessato. Il semplice fatto di entrare nell'area di ripresa della telecamera non implica che l'interessato intenda rendere pubbliche categorie particolari di dati che lo riguardano.
71. Inoltre, il trattamento di categorie particolari di dati richiede una vigilanza rafforzata e continua su taluni obblighi, ad esempio un elevato livello di sicurezza e una valutazione d'impatto sulla protezione dei dati, ove necessario.

72. Esempio Un datore di lavoro non deve utilizzare registrazioni di videosorveglianza che mostrano una manifestazione al fine di identificare gli scioperanti.

5.1 CONSIDERAZIONI GENERALI SUL TRATTAMENTO DEI DATI BIOMETRICI

73. L'uso di dati biometrici, in particolare il riconoscimento facciale, comporta maggiori rischi per i diritti degli interessati. È fondamentale che il ricorso a tali tecnologie avvenga nel dovuto rispetto dei principi di liceità, necessità, proporzionalità e minimizzazione dei dati sanciti nel RGPD. Sebbene l'uso di queste tecnologie possa essere percepito come particolarmente efficace, i titolari del trattamento dovrebbero in primo luogo valutare l'impatto sui diritti e sulle libertà fondamentali e considerare mezzi meno intrusivi per raggiungere il legittimo scopo del rispettivo trattamento.
74. Per poter configurare un trattamento di dati biometrici, secondo la definizione del RGPD, il trattamento di dati grezzi, come ad esempio le caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, deve comprendere una misurazione di tali caratteristiche. Poiché i dati biometrici sono il risultato di dette misurazioni, il RGPD afferma nel suo articolo 4, paragrafo 14, che sono dati *«[...] ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne*

consentono o confermano l'identificazione univoca [...]». Tuttavia, le riprese video di un individuo non possono essere considerate di per sé dati biometrici ai sensi dell'articolo 9, se non sono state sottoposte a un trattamento tecnico specifico per contribuire all'identificazione di tale individuo[16].

75. Affinché il trattamento sia considerato un trattamento di categorie particolari di dati personali (articolo 9), è necessario che siano trattati dati biometrici «intesi a identificare in modo univoco una persona fisica».

76. Riassumendo, alla luce dell'articolo 4, paragrafo 14, e dell'articolo 9, si devono prendere in considerazione tre criteri:

- **natura dei dati**: dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica;
- **mezzi e modalità del trattamento**: dati «ottenuti da un trattamento tecnico specifico»;
- **finalità del trattamento**: i dati devono essere utilizzati al fine di identificare in modo univoco una persona fisica.

77. L'uso della videosorveglianza associata alla funzionalità del riconoscimento biometrico da parte di soggetti privati per proprie finalità (ad esempio, marketing, statistiche o persino sicurezza) richiederà, nella maggior parte dei casi, il consenso esplicito di tutti gli interessati (articolo 9, paragrafo 2, lettera a), ma potrebbe essere applicabile anche un'altra deroga idonea di cui all'articolo 9.

78. Esempio Per migliorare il servizio, un'impresa privata sostituisce i posti di controllo per l'identificazione dei passeggeri all'interno di un aeroporto (consegna bagagli, imbarco) con sistemi di videosorveglianza che utilizzano tecniche di riconoscimento facciale per verificare l'identità dei passeggeri che hanno scelto di acconsentire a tale procedura. Poiché il trattamento rientra nel campo di applicazione dell'articolo 9, i passeggeri che avranno precedentemente prestato il consenso esplicito e informato dovranno registrarsi, ad esempio, presso un terminale automatico per creare e registrare il rispettivo modello facciale associato alla carta d'imbarco e al documento d'identità. I posti di controllo con riconoscimento facciale devono essere mantenuti chiaramente separati: ad esempio, il sistema deve essere installato all'interno di un varco di sicurezza, in modo da non acquisire i modelli biometrici delle persone che non hanno prestato il consenso. Solo i passeggeri che avranno preventivamente prestato il loro consenso e proceduto alla registrazione utilizzeranno il varco dotato del sistema biometrico.

    Esempio Un titolare del trattamento gestisce l'accesso al proprio edificio utilizzando un metodo di riconoscimento facciale. L'utilizzo di questa modalità di accesso è possibile solo se gli interessati hanno preventivamente prestato il loro consenso informato ed esplicito (ai sensi dell'articolo 9, paragrafo 2, lettera a)).

Tuttavia, al fine di garantire che non vengano acquisiti i dati di coloro che non abbiano precedentemente prestato il consenso, il riconoscimento facciale dovrebbe essere attivato dall'interessato stesso, ad esempio premendo un pulsante. Per assicurare la liceità del trattamento, il titolare deve sempre offrire una modalità alternativa di accesso all'edificio senza trattamento biometrico, ad esempio tramite badge o chiavi.

79. In questi casi, in cui vengono generati modelli biometrici, i titolari del trattamento devono garantire che, una volta ottenuta una corrispondenza o non corrispondenza, tutti i modelli intermedi realizzati in tempo reale (con il consenso esplicito e informato dell'interessato) al fine del raffronto con quelli creati dagli interessati all'atto della registrazione, siano cancellati immediatamente e in modo sicuro. I modelli creati per la registrazione dovrebbero essere conservati esclusivamente per la realizzazione della finalità del trattamento e non dovrebbero essere conservati né archiviati.

80. Tuttavia, quando la finalità del trattamento è, ad esempio, distinguere fra categorie di persone anziché identificare in modo univoco una specifica persona, il trattamento non è disciplinato dall'articolo 9.

81. Esempio Il proprietario di un esercizio commerciale vorrebbe personalizzare la propria pubblicità in base al genere e all'età dei clienti, acquisendo tali caratteristiche attraverso un sistema di videosorveglianza. Se tale sistema non genera modelli biometrici al fine di identificare in modo univoco le persone, ma semplicemente rileva tali caratteristiche fisiche al fine di classificare le persone, il trattamento non ricade nel campo di applicazione dell'articolo 9 (purché non siano trattate altre categorie particolari di dati).

82. Tuttavia, l'articolo 9 si applica se il titolare del trattamento conserva i dati biometrici (comunemente attraverso modelli creati estraendo le caratteristiche chiave dalla forma grezza dei dati biometrici, ad esempio misurazioni facciali ricavate da un'immagine), al fine di identificare in modo univoco una persona. Se un titolare del trattamento desidera individuare un interessato che rientra nella zona sorvegliata o entra in un'altra zona (ad esempio, per proiettare annunci pubblicitari personalizzati in modo continuo), in questo caso lo scopo sarebbe quello di identificare in modo univoco una persona fisica e quindi l'operazione rientrerebbe fin dall'inizio nel campo di applicazione dell'articolo 9. Ciò potrebbe accadere se il titolare conserva i modelli generati per fornire ulteriore pubblicità personalizzata su diversi cartelloni pubblicitari in vari punti all'interno del negozio. Poiché il sistema utilizza caratteristiche fisiche per individuare soggetti specifici che tornano nell'area di ripresa della telecamera (come i visitatori di un centro commerciale) e li traccia, questa funzione costituirebbe un metodo di identificazione biometrica perché è finalizzata al riconoscimento attraverso l'uso di un trattamento tecnico specifico.

83. Esempio Un negoziante ha installato un sistema di riconoscimento facciale all'interno del proprio negozio al fine di personalizzare la pubblicità rivolta ai clienti. Il titolare del trattamento deve ottenere il consenso esplicito e informato di tutti gli interessati prima di utilizzare questo sistema biometrico e trasmettere pubblicità personalizzata. Il sistema sarebbe illegale se acquisisse i dati dei visitatori o dei passanti che non hanno acconsentito alla creazione di un modello biometrico, anche se quest'ultimo venisse eliminato nel più breve tempo possibile. Infatti, questi modelli temporanei costituiscono dati biometrici trattati al fine di identificare in modo univoco una persona che potrebbe non voler ricevere pubblicità mirata.

84. Il comitato europeo per la protezione dei dati osserva che alcuni sistemi biometrici sono installati in ambienti non controllati[17], il che significa che il sistema comporta l'acquisizione in tempo reale dei volti di qualsiasi individuo che entra nell'area di ripresa della telecamera, comprese le persone che non hanno acconsentito al dispositivo biometrico, con la successiva creazione di modelli biometrici. Questi modelli vengono confrontati con quelli creati dagli interessati che hanno prestato il previo consenso durante un processo di registrazione (vale a dire gli utenti del dispositivo biometrico) al fine di consentire al titolare del trattamento di riconoscere se la persona utilizzi o meno il dispositivo biometrico. In questo caso, il sistema è spesso progettato per distinguere i soggetti da riconoscere fra quelli inseriti in una banca dati rispetto ai soggetti non registrati. Poiché lo scopo è quello di identificare in modo univoco persone fisiche, è comunque necessaria l'applicazione di una delle deroghe di cui all'articolo 9, paragrafo 2, del RGPD per trattare i dati di chiunque sia ripreso dalla telecamera.

85. Esempio Un hotel utilizza la videosorveglianza per avvisare automaticamente il direttore dell'arrivo di un VIP nel momento in cui il volto dell'ospite viene riconosciuto. I VIP in questione hanno prestato preventivamente il consenso esplicito all'uso del riconoscimento facciale, prima di essere registrati in una banca dati istituita a tale scopo. Questi sistemi di trattamento di dati biometrici sarebbero illegali a meno che tutti gli altri ospiti monitorati (al fine di identificare i VIP) abbiano acconsentito al trattamento ai sensi dell'articolo 9, paragrafo 2, lettera a), del RGPD.

    Esempio Un titolare del trattamento installa un sistema di videosorveglianza con riconoscimento facciale all'ingresso della sala da concerti da lui gestita. Il titolare deve predisporre ingressi chiaramente separati: uno provvisto del sistema biometrico e uno senza (dove, ad esempio, si esegue la scansione di un biglietto). Gli ingressi dotati di dispositivi biometrici devono essere installati e resi accessibili in modo da impedire al sistema di acquisire modelli biometrici di spettatori non consenzienti.

86. Infine, quando il consenso è richiesto dall'articolo 9 del RGPD, il titolare del trattamento non deve condizionare l'accesso ai propri servizi all'accettazione del trattamento biometrico. In altre parole, in particolare quando il trattamento biometrico è utilizzato a fini di autenticazione, il titolare del trattamento deve offrire una soluzione alternativa che non comporti il trattamento biometrico, senza imporre restrizioni o costi aggiuntivi all'interessato. Tale soluzione alternativa è necessaria anche per le persone che non possono rispettare i vincoli del dispositivo biometrico (registrazione o lettura dei dati biometrici impossibile, situazione di disabilità che ne rende difficile l'utilizzo, ecc.), e in previsione dell'indisponibilità del dispositivo biometrico (ad esempio, in caso di malfunzionamento del dispositivo) deve essere attuata una «soluzione di backup», limitata tuttavia a un uso eccezionale, a garanzia della continuità del servizio proposto. In casi eccezionali, potrebbe verificarsi una situazione in cui il trattamento dei dati biometrici è l'attività principale di un servizio fornito per contratto, ad esempio un museo che allestisce una mostra per dimostrare l'uso di un dispositivo di riconoscimento facciale, nel qual caso l'interessato non potrà rifiutare il trattamento dei dati biometrici se desidera partecipare alla mostra. In questo caso, il consenso richiesto ai sensi dell'articolo 9 resta valido se sono soddisfatti i requisiti di cui all'articolo 7.

5.2 MISURE PROPOSTE PER RIDURRE AL MINIMO I RISCHI DURANTE IL TRATTAMENTO DI DATI BIOMETRICI

87. Nel rispetto del principio della minimizzazione dei dati, i titolari del trattamento devono garantire che i dati estratti da un'immagine digitale per costruire un modello non saranno eccedenti e conterranno soltanto le informazioni necessarie per la finalità specificata, evitando così ogni possibile trattamento ulteriore. Occorre adottare misure per garantire che i modelli non possano essere trasferiti tra diversi sistemi biometrici.

88. È probabile che l'identificazione e l'autenticazione/la verifica richiedano la conservazione del modello da utilizzare per i successivi raffronti. Il titolare del trattamento deve valutare quale sia il luogo più appropriato per la conservazione dei dati. In un ambiente sotto controllo (corridoi delimitati o posti di controllo), i modelli devono essere conservati su un singolo dispositivo in possesso dell'utente e sotto il suo esclusivo controllo (in uno smartphone o nella carta d'identità) oppure – se necessario per scopi specifici e in presenza di esigenze oggettive – in una banca dati centralizzata in forma cifrata con una chiave segreta nota esclusivamente alla persona interessata, per impedire l'accesso non autorizzato al modello o al luogo ove viene conservato. Se il titolare del trattamento non può evitare di accedere ai modelli, deve adottare le opportune misure per garantire la sicurezza dei dati conservati. Può, ad esempio, cifrare il modello utilizzando un algoritmo di cifratura.

89. In ogni caso, il titolare del trattamento deve prendere tutte le precauzioni necessarie per preservare la disponibilità, l'integrità e la riservatezza dei dati

trattati. A tal fine, il responsabile del trattamento deve adottare, in particolare, le seguenti misure: trasmettere e conservare i dati in forma compartimentalizzata, conservare modelli biometrici e dati grezzi o dati di identità in banche dati distinte, cifrare i dati biometrici, in particolare i modelli biometrici, e definire una politica per la cifratura e la gestione delle chiavi, prevedere una misura organizzativa e tecnica per il rilevamento delle frodi, associare un codice di integrità ai dati (ad esempio, firma o codice hash) e vietare qualsiasi accesso esterno ai dati biometrici. Tali misure dovranno evolversi con il progredire delle tecnologie.

90. Inoltre, i titolari del trattamento dovrebbero procedere alla cancellazione dei dati grezzi (immagini del volto, segnali vocali, portamento, ecc.) e garantire l'efficacia di tale cancellazione. Se non esiste più una base giuridica per il trattamento, i dati grezzi devono essere cancellati. Infatti, nella misura in cui i modelli biometrici derivano da tali dati, si può ritenere che la costituzione di database contenenti questi dati potrebbe rappresentare una minaccia analoga se non addirittura maggiore (mentre non sempre è facile leggere un modello biometrico senza sapere come è stato programmato, i dati grezzi sono gli elementi costitutivi di qualsiasi modello). Nel caso in cui il titolare del trattamento debba conservare tali dati, è necessario valutare l'impiego di metodiche basate sull'applicazione di rumore additivo (come la filigrana digitale), che impedirebbero la creazione del modello. Il titolare del trattamento deve inoltre cancellare i dati biometrici e i modelli in caso di accesso non autorizzato al terminale di lettura e raffronto o al server di conservazione, e cancellare qualsiasi dato non utile ai fini di un trattamento ulteriore al termine della vita utile del dispositivo biometrico.

6. DIRITTI DELL'INTERESSATO

91. Data la natura del trattamento dei dati associato all'impiego della videosorveglianza, necessitano chiarimenti ulteriori su alcuni diritti dell'interessato a norma del RGPD. Questo capitolo non è tuttavia esaustivo in quanto tutti i diritti sanciti dal RGPD si applicano al trattamento dei dati personali tramite videosorveglianza.

6.1 DIRITTO DI ACCESSO

92. Un interessato ha diritto di ottenere dal titolare del trattamento la conferma o meno del fatto che i propri dati personali siano oggetto di trattamento. Per quanto riguarda la videosorveglianza, ciò significa che se nessun dato è conservato o trasferito, una volta trascorso il momento del monitoraggio in tempo reale, il titolare potrebbe soltanto comunicare che nessun dato personale è più oggetto di trattamento (oltre alle informazioni generali obbligatorie di cui all'articolo 13, si veda la *sezione 7 – Obblighi di trasparenza e informazione*). Se tuttavia i dati sono ancora in corso di trattamento al momento della ri-

chiesta (vale a dire se i dati sono conservati o trattati ininterrottamente in qualsiasi altro modo), l'interessato dovrebbe ricevere accesso e informazioni conformemente alle disposizioni dell'articolo 15.

93. Esistono, tuttavia, alcune limitazioni che in determinati casi possono trovare applicazione rispetto al diritto di accesso.

- Articolo 15, paragrafo 4, del RGPD – Ledere i diritti altrui

94. Poiché nella stessa sequenza di videosorveglianza può essere registrato un numero qualsiasi di interessati, uno screening comporterebbe un ulteriore trattamento dei dati personali di altri interessati. Se l'interessato desidera ricevere una copia del materiale (articolo 15, paragrafo 3), ciò potrebbe ledere i diritti e le libertà di altri soggetti che compaiono nella registrazione. Per evitare tale rischio, il titolare del trattamento dovrebbe quindi tenere conto del fatto che, a causa della natura intrusiva delle riprese video, in alcuni casi non dovrebbe fornire riprese video in cui siano identificabili altri interessati. Tuttavia, la protezione dei diritti di terzi non dovrebbe essere utilizzata come pretesto per impedire legittime richieste di accesso; in questi casi, il titolare del trattamento dovrebbe porre in atto misure tecniche per soddisfare la richiesta di accesso (ad esempio, modifica delle immagini tramite mascheramento o crittografia). Tuttavia, i titolari del trattamento non sono obbligati ad attuare tali misure tecniche se possono garantire in altro modo di rispondere a una richiesta ai sensi dell'articolo 15 entro il termine stabilito dall'articolo 12, paragrafo 3.

- Articolo 11, paragrafo 2, del RGPD – Il titolare del trattamento non è in grado di identificare l'interessato

95. Se nel filmato non è possibile effettuare una ricerca di dati personali (vale a dire che il titolare del trattamento probabilmente dovrebbe analizzare una grande quantità di materiale conservato per trovare l'interessato in questione), il titolare del trattamento potrebbe non essere in grado di identificare l'interessato.

96. Per questi motivi, nella sua richiesta al titolare del trattamento l'interessato dovrebbe (oltre a identificarsi anche con un documento d'identità o di persona) specificare quando – entro un lasso di tempo ragionevole in proporzione alla quantità di interessati registrati – è entrato nella zona sorvegliata. Il titolare del trattamento dovrebbe notificare preventivamente all'interessato di quali informazioni ha bisogno per poter soddisfare la richiesta. Se il titolare del trattamento può dimostrare di non essere in grado di identificare l'interessato, ne informa quest'ultimo, ove possibile. In un caso del genere, il titolare del trattamento dovrebbe informare l'interessato nella risposta circa la zona specificamente soggetta a sorveglianza, la verifica delle telecamere in uso, ecc., in modo che l'interessato comprenda esattamente quali dei suoi dati personali possano essere stati trattati.

97. Esempio Qualora l'interessato richieda una copia dei propri dati personali trattati mediante videosorveglianza all'ingresso di un centro

commerciale con 30 000 visitatori al giorno, deve specificare quando ha acceduto alla zona monitorata indicando una finestra di circa un'ora. Se il titolare del trattamento sta ancora trattando il materiale, dovrebbe fornirgli una copia del filmato. Se altri interessati possono essere identificati nello stesso materiale, allora quella parte del materiale deve essere anonimizzata (ad esempio sfocando la copia o parti di essa) prima che la copia sia consegnata all'interessato che ha presentato la richiesta.

Esempio Se il titolare del trattamento cancella automaticamente tutte le riprese, ad esempio entro due giorni, non sarà in grado di fornire le riprese all'interessato dopo tale lasso di tempo. Se il titolare del trattamento riceve una richiesta successivamente, l'interessato dovrebbe esserne informato di conseguenza.

- Articolo 12 del RGPD – Richieste eccessive

98. In caso di richieste eccessive o manifestamente infondate da parte di un interessato, il titolare del trattamento può addebitare un contributo spese ragionevole a norma dell'articolo 12, paragrafo 5, lettera a), del RGPD, o rifiutarsi di dare seguito alla richiesta (articolo 12, paragrafo 5, lettera b), del RGPD). Il titolare del trattamento deve essere in grado di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

6.2 DIRITTO ALLA CANCELLAZIONE E DIRITTO DI OPPOSIZIONE

6.2.1. DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

99. Se il titolare del trattamento continua a trattare dati personali al di là del monitoraggio in tempo reale (ad esempio, conservandoli), l'interessato può chiedere la cancellazione dei dati personali ai sensi dell'articolo 17 del RGPD.

100. Su richiesta, il titolare del trattamento è tenuto a cancellare i dati personali senza ingiustificato ritardo se sussiste una delle circostanze elencate all'articolo 17, paragrafo 1, del RGPD (e non si applica alcuna delle eccezioni elencate all'articolo 17, paragrafo 3, del RGPD). Ciò comprende l'obbligo di cancellare i dati personali quando non sono più necessari per lo scopo per cui sono stati inizialmente conservati o quando il trattamento è illecito (si veda anche la sezione 8 – Periodi di conservazione e obbligo di cancellazione). Inoltre, a seconda della base giuridica del trattamento, i dati personali dovrebbero essere cancellati:

- *Per quanto riguarda il consenso*, ogni volta che il consenso viene revocato (e non vi è altra base giuridica per il trattamento)
- per quanto riguarda il *legittimo interesse*:
  - ogniqualvolta l'interessato esercita il diritto di opposizione (cfr. la sezione 6.2.2) e non sussistano motivi legittimi cogenti e pre-

valenti per il trattamento, oppure
- in caso di marketing diretto (compresa la profilazione) ogniqualvolta gli interessati si oppongono al trattamento.

101. Se il titolare del trattamento ha reso pubbliche le riprese video (ad esempio, trasmissione o streaming online), è necessario adottare misure ragionevoli per informare altri titolari (che stanno attualmente trattando i dati personali in questione) della richiesta ai sensi dell'articolo 17, paragrafo 2, del RGPD. Le misure ragionevoli dovrebbero comprendere misure tecniche che tengano conto della tecnologia disponibile e dei costi di implementazione. Nella misura del possibile, il titolare del trattamento dovrebbe informare – in caso di cancellazione dei dati personali – qualunque soggetto al quale siano stati precedentemente comunicati tali dati, conformemente a quanto disposto nell'articolo 19 del RGPD.

102. Oltre all'obbligo di cancellare i dati personali su richiesta dell'interessato, il titolare del trattamento è tenuto, in virtù dei principi generali del RGPD, a limitare i dati personali conservati (si veda la sezione 8).

103. Rispetto alla videosorveglianza vale la pena osservare, ad esempio, che offuscando l'immagine senza alcuna possibilità di recuperare successivamente i dati personali precedentemente contenuti in tale immagine , si deve ritenere che i dati personali siano stati cancellati in conformità delle disposizioni del RGPD.

104. Esempio Un minimarket ha subito atti vandalici, in particolare sull'esterno del negozio, e utilizza quindi la videosorveglianza al di fuori dell'entrata, con la telecamera che riprende l'area prossima alle pareti. Un passante chiede che vengano cancellati i suoi dati personali a partire da quel momento. Il titolare del trattamento è tenuto a rispondere alla richiesta senza ingiustificato ritardo e al più tardi entro un mese. Poiché il filmato in questione non soddisfa più lo scopo per il quale è stato inizialmente conservato (non si è verificato alcun atto vandalico durante il periodo in cui l'interessato è transitato nei pressi del negozio), al momento della richiesta non vi è alcun interesse legittimo a conservare i dati tale da prevalere sugli interessi degli interessati. Il titolare del trattamento deve cancellare i dati personali.

6.2.2 DIRITTO DI OPPOSIZIONE

105. Rispetto alla videosorveglianza basata su un legittimo interesse (articolo 6, paragrafo 1, lettera f), del RGPD), o con riguardo alla necessità nello svolgimento di un compito di interesse pubblico (articolo 6, paragrafo 1, lettera e), del RGPD) l'interessato ha il diritto di opporsi al trattamento in qualsiasi momento, per motivi connessi alla sua situazione particolare, ai sensi dell'articolo 21 del RGPD. A meno che il titolare del trattamento possa

dimostrare l'esistenza di motivi legittimi cogenti che prevalgono sui diritti e sugli interessi dell'interessato, il trattamento dei dati della persona che vi si è opposta deve cessare. Il titolare è tenuto a rispondere alle richieste dell'interessato senza ingiustificato ritardo e al più tardi entro un mese.

106. Nel contesto della videosorveglianza, tale opposizione potrebbe essere formulata all'ingresso, durante il periodo di permanenza nella zona sorvegliata o dopo l'uscita dalla stessa. In pratica ciò significa che, a meno che il titolare del trattamento abbia motivi legittimi cogenti, la sorveglianza di una zona in cui potrebbero essere identificate persone fisiche è lecita unicamente se:

(1) il titolare è in grado di interrompere immediatamente, su richiesta, il trattamento dei dati personali da parte della telecamera, o

(2) la zona sorvegliata è soggetta a restrizioni tali da consentire al titolare del trattamento di ottenere il consenso dell'interessato prima che questi vi acceda e non è una zona a cui l'interessato in quanto cittadino ha diritto di accedere.

107. Le presenti linee guida non mirano a identificare ciò che è considerato un legittimo interesse cogente (articolo 21 del RGPD).

108. Quando si utilizza la videosorveglianza per finalità di marketing diretto, l'interessato ha il diritto di opporsi al trattamento a sua discrezione; il diritto di opposizione, infatti, è assoluto in tale contesto (articolo 21, paragrafi 2 e 3, del RGPD).

109. Esempio Un minimarket ha subito atti vandalici, in particolare sull'esterno del negozio, e utilizza quindi la videosorveglianza al di fuori dell'entrata, con la telecamera che riprende l'area prossima alle pareti. Un passante chiede che vengano cancellati i suoi dati personali a partire da quel momento. Il titolare del trattamento è tenuto a rispondere alla richiesta senza ingiustificato ritardo e al più tardi entro un mese. Poiché il filmato in questione non soddisfa più lo scopo per il quale è stato inizialmente conservato (non si è verificato alcun atto vandalico durante il periodo in cui l'interessato è transitato nei pressi del negozio), al momento della richiesta non vi è alcun interesse legittimo a conservare i dati tale da prevalere sugli interessi degli interessati. Il titolare del trattamento deve cancellare i dati personali.

7. OBBLIGHI DI TRASPARENZA E INFORMAZIONE[18]

110. La normativa europea in materia di protezione dei dati dispone da tempo che gli interessati debbano essere consapevoli del fatto che è in funzione un sistema di videosorveglianza. Dovrebbero essere informati in modo dettagliato sui luoghi sorvegliati[19]. A norma del RGPD gli obblighi gene-

rali di trasparenza e informazione sono sanciti dall'articolo 12 e seguenti del RGPD. Le «Linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679 (WP260)» del gruppo di lavoro "Articolo 29", approvate dal comitato europeo per la protezione dei dati il 25 maggio 2018, forniscono ulteriori dettagli. In linea con il punto 26 del WP260, è l'articolo 13 del RGPD che si applica se i dati personali sono raccolti «[...] presso l'interessato mediante osservazione (ad es. utilizzando dispositivi o software per catturare dati in modo automatizzato quali telecamere, [...])».

111. Alla luce della quantità di informazioni da fornire all'interessato, i titolari del trattamento possono seguire un approccio scalare, optando per una combinazione di metodi al fine di assicurare la trasparenza (WP260, punto 35; WP89, punto 22). Per quanto riguarda la videosorveglianza, le informazioni più importanti devono essere indicate sul segnale di avvertimento stesso (primo livello), mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello).

7.1 INFORMAZIONI DI PRIMO LIVELLO (SEGNALETICA DI AVVERTIMENTO)

112. Il primo livello riguarda la modalità con cui avviene la prima interazione fra il titolare del trattamento e l'interessato. In questa fase, i titolari del trattamento possono utilizzare un segnale di avvertimento che indichi le informazioni pertinenti. Tali informazioni possono essere fornite in combinazione con un'icona per dare, in modo ben visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto (articolo 12, paragrafo 7, del RGPD). Il formato delle informazioni dovrà adeguarsi alle varie ubicazioni (WP89, punto 22).

7.1.1. POSIZIONAMENTO DELLA SEGNALETICA DI AVVERTIMENTO

113. Le informazioni dovrebbero essere posizionate in modo da permettere all'interessato di riconoscere facilmente le circostanze della sorveglianza, prima di entrare nella zona sorvegliata (approssimativamente all'altezza degli occhi). Non è necessario rivelare l'ubicazione della telecamera, purché non vi siano dubbi su quali zone sono soggette a sorveglianza e sia chiarito in modo inequivocabile il contesto della sorveglianza (WP 89, punto 22). L'interessato deve poter stimare quale zona sia coperta da una telecamera in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario.

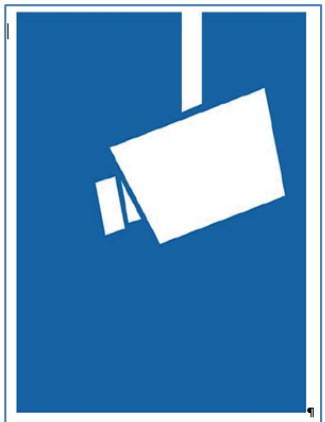
7.1.2 CONTENUTO DELLE INFORMAZIONI DI PRIMO LIVELLO

114. Generalmente, le informazioni di primo livello (segnale di avvertimento) dovrebbero comunicare i dati più importanti, ad esempio le finalità del trattamento, l'identità del titolare del trattamento e l'esistenza dei diritti

dell'interessato, unitamente alle informazioni sugli impatti più consistenti del trattamento[20]. Si può fare riferimento, ad esempio, ai legittimi interessi perseguiti dal titolare (o da un soggetto terzo) e ai recapiti del responsabile della protezione dei dati (se applicabile). Occorre anche fare riferimento alle informazioni di secondo livello, più dettagliate,, indicando dove e come trovarle.

115. Inoltre, la segnaletica deve contenere anche quelle informazioni che potrebbero risultare inaspettate per l'interessato (WP260, punto 38). Potrebbe trattarsi, ad esempio, della trasmissione di dati a terzi, in particolare se ubicati al di fuori dell'UE, e del periodo di conservazione. Se tali informazioni non sono indicate, l'interessato dovrebbe poter confidare nel fatto che vi sia solo una sorveglianza in tempo reale (senza alcuna registrazione di dati o trasmissione a soggetti terzi).

116. Esempio (suggerimento non vincolante)



Identità del titolare del trattamento e, ove applicabile, del suo rappresentante;

Recapiti, anche del responsabile della protezione dei dati (ove applicabile);

Informazioni sul trattamento che ha il maggiore impatto sull'interessato (ad esempio, periodo di conservazione o monitoraggio in tempo reale, pubblicazione o trasmissione di filmati a soggetti terzi);

Scopo(i) della videosorveglianza:

Ulteriori informazioni sono disponibili:
- a mezzo comunicazione
- presso la nostra reception/nelle informazioni al cliente/nel registro
- via Internet (URL)...

Diritti degli interessati: Gli interessati possono esercitare diversi diritti tra cui, in particolare, il diritto di richiedere al titolare del trattamento l'accesso o la cancellazione dei propri dati personali.

Per maggiori dettagli su questa videosorveglianza, compresi i diritti degli interessati, si consultino le informazioni complete fornite dal titolare del trattamento utilizzando le opzioni che figurano sulla sinistra.

7.2 INFORMAZIONI DI SECONDO LIVELLO

117. Le informazioni di secondo livello devono essere facilmente accessibili per l'interessato, ad esempio attraverso un pagina informativa completa messa a disposizione in uno snodo centrale (sportello informazioni, reception, cassa, ecc.) o affissa in un luogo di facile accesso. Come sopra illustrato, la segnaletica di avvertimento di primo livello deve contenere un chiaro riferimento a tale secondo livello di informazioni. Inoltre, è preferibile che nelle informazioni di primo livello si faccia riferimento a una

fonte digitale (ad esempio, un codice QR o un indirizzo web) per le informazioni di secondo livello. Tuttavia, le informazioni dovrebbero essere facilmente disponibili anche in formato non digitale. Dovrebbe essere possibile accedere al secondo livello di informazioni senza entrare nell'area videosorvegliata, soprattutto se le informazioni sono fornite digitalmente (ad esempio, tramite un link). Un altro strumento appropriato potrebbe essere la messa a disposizione di un numero telefonico da contattare. Comunque siano fornite le informazioni, queste devono contenere tutti gli elementi obbligatori a norma dell'articolo 13 del RGPD.

118. Oltre a queste possibilità, e anche per renderle più efficaci, il comitato europeo per la protezione dei dati promuove l'uso di strumenti tecnologici per fornire informazioni agli interessati. Per esempio, si possono geolocalizzare le telecamere caricando le relative informazioni su app o siti web di mappatura, cosicché le persone possano facilmente, da un lato, identificare e specificare le fonti video in vista dell'esercizio dei propri diritti e, dall'altro lato, ottenere informazioni più dettagliate sulla tipologia di trattamento.

119. Esempio Un negoziante videosorveglia il suo esercizio commerciale. Ai fini del rispetto delle disposizioni dell'articolo 13, è sufficiente che collochi un cartello di avvertimento in un punto facilmente visibile all'ingresso dell'esercizio commerciale, contenente le informazioni di primo livello. Dovrà poi fornire le informazioni di secondo livello attraverso un foglio informativo disponibile presso la cassa o qualsiasi altro punto centrale e facilmente accessibile all'interno dell'esercizio.

8. PERIODI DI CONSERVAZIONE E OBBLIGO DI CANCELLAZIONE

120. I dati personali non possono essere conservati più a lungo di quanto necessario per le finalità per le quali sono trattati (articolo 5, paragrafo 1, lettere c) ed e), del RGPD). In alcuni Stati membri possono essere previste disposizioni specifiche per i periodi di conservazione con riguardo alla videosorveglianza a norma dell'articolo 6, paragrafo 2, del RGPD.

121. La necessità o meno di conservare i dati personali dovrebbe essere valutata entro una tempistica ristretta. In via generale, gli scopi legittimi della videosorveglianza sono spesso la protezione del patrimonio o la conservazione di elementi di prova. Solitamente è possibile individuare eventuali danni entro uno o due giorni. Per facilitare la dimostrazione di conformità al quadro normativo in materia di protezione dei dati, è nell'interesse del titolare del trattamento organizzarsi proattivamente (ad esempio nominando, se necessario, un responsabile per lo screening e la protezione del materiale video). Tenendo conto dei principi di cui all'articolo 5, paragrafo 1, lettere c) ed e), del RGPD, vale a dire la minimizzazione dei dati e la

limitazione della loro conservazione, i dati personali dovrebbero essere – nella maggior parte dei casi (ad esempio se la videosorveglianza serve allo scopo di rilevare atti vandalici) – cancellati dopo alcuni giorni, preferibilmente tramite meccanismi automatici. Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione. Se il titolare del trattamento utilizza la videosorveglianza non solo per monitorare i propri locali, ma anche per conservare i dati, deve garantire che la conservazione sia effettivamente necessaria per raggiungere lo scopo specifico. In tal caso, il periodo di conservazione deve essere definito chiaramente e specificamente con riguardo alle singole finalità. È responsabilità del titolare del trattamento definire il periodo di conservazione conformemente ai principi di necessità e proporzionalità e dimostrare la conformità alle disposizioni del RGPD.

122. Esempio Normalmente, il titolare di un piccolo esercizio commerciale si accorgerebbe di eventuali atti vandalici il giorno stesso in cui si verificassero. Un periodo di conservazione di 24 ore è quindi sufficiente. La chiusura nei fine settimana o in periodi festivi più lunghi potrebbe tuttavia giustificare un periodo di conservazione più prolungato. Se viene rilevato un danno, può essere anche necessario conservare il filmato per un periodo più lungo al fine di intraprendere un'azione legale contro l'autore del reato.

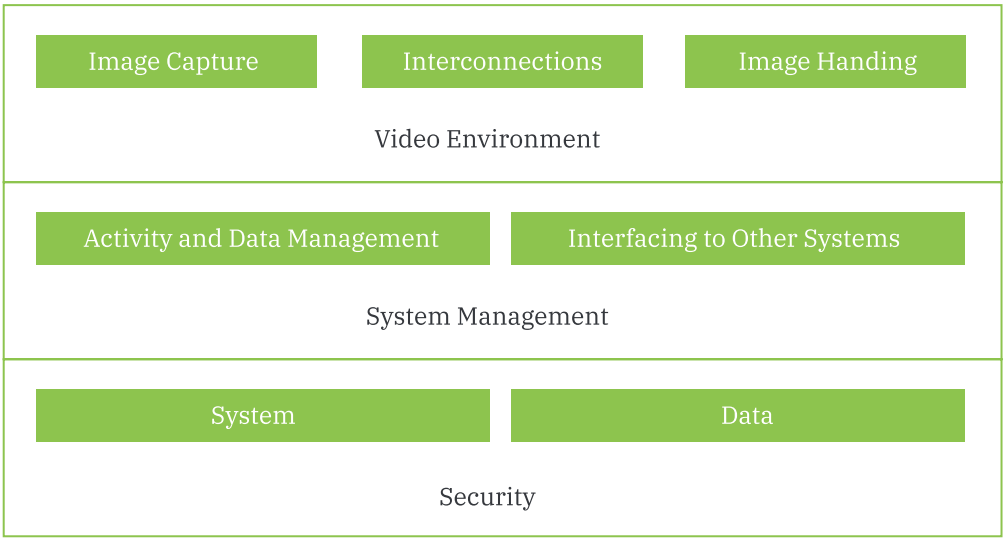
9. MISURE TECNICHE E ORGANIZZATIVE

123. Come indicato all'articolo 32, paragrafo 1, del RGPD, non è sufficiente che il trattamento di dati personali durante videosorveglianza sia lecito, in quanto titolari e responsabili del trattamento devono anche garantire l'adeguata sicurezza dei dati in questione . **Le misure tecniche** e **organizzative** attuate devono essere **proporzionate ai rischi per i diritti e le libertà delle persone fisiche** derivanti dai casi di distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso ai dati di videosorveglianza. A norma degli articoli 24 e 25 del RGPD, i titolari del trattamento devono mettere in atto misure tecniche e organizzative anche al fine di salvaguardare tutti i principi di protezione dei dati durante il trattamento e di stabilire i mezzi affinché gli interessati possano esercitare i propri diritti secondo la definizione di cui agli articoli 15-22 del RGPD. I titolari del trattamento dovrebbero adottare una struttura interna e politiche in grado di assicurare l'attuazione di tali misure sia al momento di definire i mezzi di trattamento sia all'atto del trattamento stesso, compresa l'esecuzione di valutazioni d'impatto sulla protezione dei dati ove necessario.

9.1 DESCRIZIONE GENERALE DI UN SISTEMA DI VIDEOSORVEGLIANZA

124. Un sistema di videosorveglianza (VSS)[21] è costituito da dispositivi analogici e digitali nonché da software per acquisire immagini, gestirle e mostrarle a un operatore. I suoi componenti sono categorizzabili come segue:

- Ambiente video: acquisizione immagini, interconnessioni e gestione immagini:
  - l'acquisizione delle immagini serve a generare un'immagine del mondo reale in un formato tale da poter essere utilizzata dal resto del sistema,
  - le interconnessioni comprendono tutte le trasmissioni di dati all'interno dell'ambiente video, vale a dire connessioni e comunicazioni. Esempi di connessioni sono cavi, reti digitali e trasmissioni wireless. Le comunicazioni descrivono tutti i segnali video e dati di controllo, che potrebbero essere digitali o analogici,
  - la gestione delle immagini comprende l'analisi, la conservazione e la presentazione di un'immagine o di una sequenza di immagini.
- Dal punto di vista della gestione del sistema, un VSS ha le seguenti funzioni logiche:
  - gestione dei dati e delle attività, comprendente la gestione dei comandi degli operatori e delle attività generate dal sistema (procedure di allarme, operatori di allarme),
  - le interfacce con altri sistemi potrebbero includere la connessione ad altri sistemi di sicurezza (controllo accessi, allarme antincendio) o non legati alla sicurezza (sistemi di gestione edifici, riconoscimento automatico delle targhe).
- La sicurezza di un VSS consiste nella riservatezza, nell'integrità e nella disponibilità del sistema e dei dati:
  - la sicurezza del sistema comprende la sicurezza fisica di tutti i componenti del sistema e il controllo dell'accesso al VSS,
  - la sicurezza dei dati comprende la prevenzione della perdita o della manipolazione dei dati.



125.

Image Capture	Acquisizione immagini
Interconnections	Interconnessioni
Image Handling	Gestione immagini
Video Environment	Ambiente video
Activity and Data Management	Gestione dell'attività e dei dati
Interfacing to Other Systems	Interfacciamento con altri sistemi
System Management	Gestione del sistema
System	Sistema
Data	Dati
Security	Sicurezza

Figura 1. Sistema di videosorveglianza

9.2 PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

126. Come stabilito dall'articolo 25 del RGPD, i titolari del trattamento devono mettere in atto adeguate misure tecniche e organizzative di protezione dei dati non appena pianificano l'installazione di un sistema di videosorve-

glianza, prima di iniziare la raccolta e il trattamento di filmati. Questi principi sottolineano la necessità di tecnologie integrate per il miglioramento della privacy, impostazioni predefinite che riducano al minimo il trattamento dei dati e l'adozione degli strumenti necessari ai fini della massima protezione possibile dei dati personali[22].

127. I titolari del trattamento dovrebbero integrare la protezione dei dati e la tutela della privacy non solo nelle specifiche di progettazione della tecnologia, ma anche nelle pratiche organizzative. Per quanto riguarda queste ultime, il titolare del trattamento dovrebbe adottare un piano di gestione appropriato, stabilire e applicare politiche e procedure relative alla videosorveglianza. Dal punto di vista tecnico, le specifiche e la progettazione del sistema dovrebbero includere requisiti per il trattamento dei dati personali conformemente ai principi di cui all'articolo 5 del RGPD (liceità del trattamento, limitazione della finalità e dei dati, minimizzazione dei dati per impostazione predefinita ai sensi dell'articolo 25, paragrafo 2, del RGPD, integrità e riservatezza, responsabilizzazione, ecc.). Nel caso in cui un titolare del trattamento preveda di acquistare un sistema di videosorveglianza commerciale, deve includere questi requisiti nelle specifiche di acquisto. Il titolare del trattamento deve garantire la conformità a questi requisiti, applicandoli a tutti i componenti del sistema e a tutti i dati da esso trattati, durante l'intero ciclo di vita.

9.3 ESEMPI CONCRETI DI MISURE PERTINENTI

128. La maggior parte delle misure che possono essere utilizzate per la sicurezza dei trattamenti di videosorveglianza, soprattutto quando si utilizzano apparecchiature digitali e software, sono sostanzialmente identiche alle misure utilizzate in altri sistemi informatici. Tuttavia, indipendentemente dalla soluzione prescelta, il titolare del trattamento deve proteggere adeguatamente tutti i componenti di un sistema di videosorveglianza e i dati in tutte le fasi, vale a dire durante la conservazione (dati a riposo), la trasmissione (dati in transito) e il trattamento (dati in uso). A tal fine è necessario che titolari e responsabili del trattamento combinino misure organizzative e tecniche.

129. Nel selezionare le soluzioni tecniche, il titolare del trattamento dovrebbe considerare le tecnologie che tutelano la privacy anche perché migliorano la sicurezza. Esempi di questo tipo di tecnologie sono i sistemi che consentono il mascheramento o l'offuscamento delle zone irrilevanti per la sorveglianza, oppure l'editing di immagini di terzi, quando si forniscono filmati agli interessati[23]. D'altra parte, le soluzioni individuate non dovrebbero prevedere funzioni non necessarie (ad esempio, movimento illimitato delle telecamere, capacità di zoom, radiotrasmissione, analisi e registrazioni audio). Le funzioni fornite, ma non necessarie, devono essere disattivate.

130. Su questo argomento è disponibile una vasta letteratura, comprese le norme internazionali e le specifiche tecniche sulla sicurezza fisica dei sistemi

multimediali[24] e sulla sicurezza dei sistemi informatici[25] in genere. Questa sezione fornisce quindi una panoramica di alto livello di questo argomento.

9.3.1 MISURE ORGANIZZATIVE

131. Oltre alla eventuale necessità di una valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment*, DPIA) (si veda la *sezione 10*), nell'elaborare le proprie politiche e procedure di videosorveglianza i titolari del trattamento dovrebbero prendere in considerazione gli elementi indicati di seguito.

- Responsabilità della gestione e del funzionamento del sistema di videosorveglianza.
- Finalità e ambito di applicazione del progetto di videosorveglianza.
- Utilizzo appropriato e vietato (dove e quando la videosorveglianza è consentita e dove e quando non lo è: ad esempio, uso di telecamere nascoste e registrazione audio oltre che video)[26].
- Misure di trasparenza di cui alla sezione 7 (*Obblighi di trasparenza e informazione*).
- Modalità e durata delle registrazioni video, compresa la conservazione delle videoregistrazioni relative a problemi di sicurezza.
- Chi deve seguire una formazione specifica e quando.
- Chi ha accesso alle registrazioni video e per quali scopi.
- Procedure operative (ad esempio, da chi e da dove viene monitorata la videosorveglianza, cosa fare in caso di un problema di violazione dei dati).
- Quali procedure devono seguire i soggetti esterni per richiedere le videoregistrazioni e le procedure per respingere o accogliere tali richieste.
- Procedure per l'approvvigionamento, l'installazione e la manutenzione di VSS.
- Gestione dei problemi e procedure di recupero.

9.3.2 MISURE TECNICHE

132. **Sicurezza del sistema** significa **sicurezza fisica** di tutti i componenti del sistema, nonché integrità del sistema, vale a dire **protezione e resilienza in caso di interferenze volontarie e involontarie nel suo normale funzionamento e controllo degli accessi**. Sicurezza dei dati significa **riservatezza** (i dati sono accessibili solo a coloro a cui è concesso l'accesso), **integrità** (prevenzione della perdita o della manipolazione dei dati) e **disponibilità** (i dati possono essere consultati ogniqualvolta sia necessario).

133. La **sicurezza fisica** è una parte fondamentale della protezione dei dati e costituisce la prima linea di difesa, perché protegge le apparecchiature

VSS da furti, atti vandalici, calamità naturali, catastrofi provocate dall'uomo e danni accidentali (ad esempio, sovratensioni elettriche, temperature estreme e riversamento di caffè). Nel caso di sistemi analogici, la sicurezza fisica è la più importante per la loro protezione.

134. La **sicurezza del sistema e dei dati**, vale a dire la protezione da interferenze volontarie e involontarie nel suo normale funzionamento, può comprendere:

- protezione dell'intera infrastruttura del VSS (comprese telecamere remote, cablaggio e alimentazione) contro manomissioni fisiche e furti;
- protezione della trasmissione di filmati attraverso canali di comunicazione sicuri a prova di intercettazione;
- cifratura dei dati;
- utilizzo di soluzioni basate su hardware e software quali firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici;
- rilevamento di guasti di componenti, software e interconnessioni;
- strumenti per ripristinare la disponibilità dei dati personali e l'accesso agli stessi in caso di problemi fisici o tecnici.

135. Il **controllo degli accessi** garantisce che solo le persone autorizzate possano accedere al sistema e ai dati, mentre agli altri viene impedito di farlo. Le misure che supportano il controllo fisico e logico degli accessi includono:

- la garanzia che tutti i locali in cui viene effettuato il monitoraggio mediante videosorveglianza e in cui vengono conservate le riprese video siano protetti contro l'accesso non supervisionato da parte di terzi;
- il posizionamento dei monitor (soprattutto quando si trovano in zone aperte, come una reception) in modo tale che solo gli operatori autorizzati possano visualizzarli;
- la definizione e l'applicazione delle procedure per la concessione, la modifica e la revoca dell'accesso;
- l'attuazione di metodi e mezzi di autenticazione e autorizzazione dell'utente, tra cui ad esempio la lunghezza delle password e la frequenza della loro modifica;
- la registrazione e la revisione periodica delle azioni eseguite dagli utenti (con riguardo sia al sistema sia ai dati);
- l'esecuzione del monitoraggio e l'individuazione di guasti agli accessi in modo continuativo e la risoluzione in tempi brevi delle carenze individuate.

10. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

136. Ai sensi dell'articolo 35, paragrafo 1, del RGPD, i titolari del trattamento sono tenuti a condurre valutazioni d'impatto sulla protezione dei dati quando una determinata tipologia di trattamenti può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. L'articolo 35, paragrafo 3, lettera c), del RGPD stabilisce che i titolari del trattamento sono tenuti a effettuare valutazioni d'impatto sulla protezione dei dati se il trattamento consiste nella sorveglianza sistematica di una zona accessibile al pubblico su larga scala. Inoltre, ai sensi dell'articolo 35, paragrafo 3, lettera b), del RGPD, è necessaria una valutazione d'impatto sulla protezione dei dati anche quando il titolare intende trattare categorie particolari di dati su larga scala.

137. Le linee guida in materia di valutazione d'impatto sulla protezione dei dati[27] forniscono ulteriori indicazioni ed esempi più dettagliati relativi alla videosorveglianza (ad esempio, per quanto riguarda «l'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade»). L'articolo 35, paragrafo 4, del RGPD prevede che ogni autorità di controllo pubblichi un elenco delle tipologie di trattamento soggette obbligatoriamente a valutazione d'impatto sulla protezione dei dati nel rispettivo Stato membro. Di norma, questi elenchi sono reperibili sui siti web delle autorità. Date le finalità tipiche della videosorveglianza (protezione delle persone e dei beni, individuazione, prevenzione e controllo di reati, raccolta di elementi di prova e identificazione biometrica di soggetti sospetti), è ragionevole supporre che molti casi di videosorveglianza richiederanno una valutazione d'impatto sulla protezione dei dati. I titolari del trattamento dovrebbero quindi consultare attentamente questi documenti al fine di determinare se tale valutazione sia necessaria e, in tal caso, al fine di effettuarla. L'esito della valutazione d'impatto sulla protezione dei dati dovrebbe determinare la scelta del titolare del trattamento sulle misure di protezione dei dati implementate.

138. È inoltre importante ricordare che, ove i risultati della valutazione d'impatto sulla protezione dei dati indichino che il trattamento comporterebbe un rischio elevato nonostante le misure di sicurezza pianificate dal titolare, occorrerà consultare l'autorità di controllo competente prima di procedere al trattamento. Le disposizioni in materia di consultazioni preventive sono contenute nell'articolo 36 del RGPD.

Per il comitato europeo per la protezione dei dati
La presidente

(Andrea Jelinek)

NOTE

[1] Nel presente parere con il termine «Stati membri» si intendono gli «Stati membri del SEE».

[2] Il comitato europeo per la protezione dei dati osserva che, laddove il RGPD lo consenta, potrebbero applicarsi requisiti specifici nella legislazione nazionale.

[3] Cfr. anche il considerando 18.

[4] Corte di giustizia dell'Unione europea, sentenza nella causa C-101/01, *Bodil Lindqvist*, 6 novembre 2003, punto 47.

[5] Corte di giustizia dell'Unione europea, sentenza nella causa C-212/13, *František Ryneš contro Úřad pro ochranu osobních údajů*, 11 dicembre 2014, punto 33.

[6] Le norme sulla raccolta di prove nei procedimenti civili variano da uno Stato membro all'altro.

[7] Le presenti linee guida non analizzano né approfondiscono la normativa nazionale che potrebbe differire da uno Stato membro all'altro.

[8] Corte di giustizia dell'Unione europea, sentenza nella causa C-13/16, *Rīgas satiksme*, 4 maggio 2017

[9] Cfr. WP217, gruppo di lavoro "Articolo 29".

[10] Cfr. WP217, Gruppo di lavoro "Articolo 29", pag. 24 e segg. Cfr. anche la causa C-708/18 della Corte di giustizia dell'Unione europea, punto 44.

[11] In alcuni Stati membri ciò potrebbe anche essere soggetto alla normativa nazionale.

[12] Cfr. anche: Gruppo di lavoro "Articolo 29", parere 2/2017 sul trattamento dei dati sul luogo di lavoro, WP 249, adottato l'8 giugno 2017.

[13] La base su cui si fonda il trattamento dei dati in questione deve essere stabilita dal diritto dell'Unione o dal diritto degli Stati membri ed è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (articolo 6, paragrafo 3).

[14] Gruppo di lavoro "Articolo 29": «Linee guida sul consenso ai sensi del regolamento (UE) 2016/679» (WP 259 rev. 01) – approvate dal comitato europeo per la protezione dei dati.

[15] Gruppo di lavoro "Articolo 29", «Linee guida sul consenso ai sensi del regolamento (UE) 2016/679» (WP 259) – approvate dal comitato europeo per la protezione dei dati – di cui si dovrebbe tener conto.

[16] Il considerando 51 del RGPD supporta quest'analisi affermando che *«[...] Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica. [...]».*

[17] Significa che il dispositivo biometrico è ubicato in uno spazio aperto al pubblico ed è in grado di funzionare su chiunque passi di lì, al contrario dei sistemi biometrici in ambienti controllati, che possono essere utilizzati soltanto con la partecipazione di una persona consenziente.

[18] Potrebbero essere applicabili disposizioni specifiche della normativa nazionale.

[19] Cfr. il WP89, parere 4/2004 relativo al trattamento dei dati personali mediante videosorveglianza del gruppo di lavoro dell'articolo 29).

[20] Cfr. il WP260, punto 38.

[21] Il RGPD non definisce i sistemi di videosorveglianza; una descrizione tecnica è disponibile ad esempio nella norma EN 62676-1-1:2014 Sistemi di videosorveglianza per l'uso in applicazioni di sicurezza – Parte 1-1: requisiti del sistema video

[22] WP 168, Parere sul tema «Il futuro della privacy», contributo congiunto del gruppo di lavoro "Articolo 29" e del gruppo di lavoro «Polizia e giustizia» alla consultazione della Commissione europea sul quadro giuridico per il diritto fondamentale alla protezione dei dati personali (adottato il 1º dicembre 2009).

[23] L'uso di tali tecnologie può anche essere obbligatorio in alcuni casi al fine di osservare le disposizioni di cui all'articolo 5, paragrafo 1, lettera c). In ogni caso, può servire da esempio di buone prassi.

[24] IEC TS 62045 – Sicurezza multimediale – Linee guida per la protezione della privacy di apparecchiature e sistemi in uso e fuori uso.

[25] ISO/IEC 27000:2013 – Sistemi di gestione per la sicurezza delle informazioni.

[26] Ciò può dipendere dalle leggi nazionali e dalle normative settoriali.

[27] WP 248 rev.01, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento «possa presentare un rischio elevato» ai fini del regolamento (UE) 2016/679 – approvate dal Comitato europeo per la protezione dei dati.

Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita Versione 2.0

Adottate il 20 ottobre 2020

Cronologia delle versioni

Versione 1.0	13 novembre 2019	Adozione delle linee guida per consultazione pubblica
Versione 2.0	20 ottobre 2020	Adozione delle linee guida da parte dell'EDPB dopo la consultazione pubblica

Indice

1 Ambito di applicazione

2 Analisi dell'articolo 25, paragrafi 1 e 2: protezione dei dati fin dalla progettazione e protezione per impostazione predefinita
- 2.1 Articolo 25, paragrafo 1: protezione dei dati fin dalla progettazione
  - 2.1.1 Obbligo del titolare del trattamento di attuare misure tecniche e organizzative adeguate e le necessarie garanzie nel trattamento
  - 2.1.2 Volte ad attuare i principi di protezione dei dati in modo efficace e tutelare i diritti e le libertà degli interessati
  - 2.1.3 Elementi di cui tenere conto
  - 2.1.4 Aspetto temporale
- 2.2 Articolo 25, paragrafo 2: protezione dei dati per impostazione predefinita
  - 2.2.1 Siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento
  - 2.2.2 Perimetro dell'obbligo di minimizzazione dei dati

3 Attuazione dei principi di protezione nel trattamento dei dati personali utilizzando la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita
- 3.1 Trasparenza
- 3.2 Liceità
- 3.3 Correttezza
- 3.4 Limitazione delle finalità
- 3.5 Minimizzazione dei dati
- 3.6 Esattezza
- 3.7 Limitazione della conservazione
- 3.8 Integrità e riservatezza
- 3.9 Responsabilizzazione

4 Articolo 25, paragrafo 3: certificazione

5 Misure prese in attuazione dell'Articolo 25 e relative conseguenze

6 Raccomandazioni

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in appresso: il «RGPD»),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificato dalla decisione del comitato misto SEE n. 154/2018, del 6 luglio 2018,

visto l'articolo 12 e l'articolo 22 del proprio regolamento interno,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

SINTESI

In un mondo sempre più digitale, il rispetto dei requisiti della protezione dei dati fin dalla progettazione e della protezione per impostazione predefinita svolge un ruolo cruciale nel promuovere la tutela della vita privata e la protezione dei dati nella società. È pertanto fondamentale che i titolari del trattamento prendano sul serio questa responsabilità e si attengano agli obblighi del RGPD quando progettano i rispettivi trattamenti.

Le presenti linee guida forniscono orientamenti generali sull'obbligo di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita (in appresso «DPbDD») stabilito dall'articolo 25 del RGPD. La DPbDD costituisce un obbligo per tutti i titolari del trattamento, indipendentemente dalle dimensioni e dalla complessità del trattamento stesso. Per poter attuare la DPbDD, è di cruciale importanza che il titolare comprenda i principi della protezione dei dati nonché i diritti e le libertà dell'interessato.

L'obbligo principale consiste nel predisporre misure adeguate e garanzie necessarie che permettano *un'attuazione efficace dei principi della protezione dei dati e, di conseguenza, dei diritti e delle libertà degli interessati fin dalla progettazione e per impostazione predefinita*. L'articolo 25 prescrive gli elementi, sia della progettazione che dell'impostazione predefinita, di cui occorre tenere conto. Tali elementi saranno ulteriormente sviluppati nelle presenti linee guida.

L'articolo 25, paragrafo 1, prevede che il titolare debba prendere in considerazione la DPbDD fin dalla pianificazione di un nuovo trattamento. I titolari attuano la DPbDD *prima* del trattamento e poi *costantemente* durante il trattamento, verificando regolarmente l'efficacia delle misure e delle garanzie individuate. La DPbDD si applica altresì a sistemi preesistenti che trattino dati personali.

Le linee guida contengono inoltre indicazioni per un'efficace attuazione dei principi di protezione dei dati di cui all'articolo 5, elencando gli elementi chiave della progettazione e dell'impostazione predefinita nonché casi pratici a titolo illustrativo. Il titolare deve valutare l'adeguatezza delle misure consigliate nel contesto dello specifico trattamento.

L'EDPB fornisce raccomandazioni su come i titolari del trattamento, i responsabili del trattamento e i produttori possano cooperare per attuare la DPbDD. In particolare, incoraggia i titolari del trattamento nei singoli settori, i responsabili del trattamento e i produttori ad avvalersi della DPbDD quale strumento per conseguire un vantaggio competitivo nella commercializzazione dei rispettivi prodotti presso i titolari del trattamento e gli interessati, oltre a incoraggiare tutti i titolari del trattamento a servirsi di certificazioni e codici di condotta.

1. AMBITO DI APPLICAZIONE

1. Le linee guida sono incentrate sull'attuazione, da parte dei titolari del trattamento, della DPbDD in virtù dell'obbligo di cui all'articolo 25 del RGPD[1]. Anche altri attori, quali i responsabili del trattamento e i produttori di prodotti, servizi e applicazioni (in prosieguo: «produttori»), che non sono direttamente contemplati dall'articolo 25, possono trovare utili queste linee guida in vista della creazione di prodotti e servizi conformi al RGPD che consentano ai titolari del trattamento di adempiere ai propri obblighi in materia di protezione dei dati[2]. Il considerando 78 del RGPD aggiunge che la DPbDD dovrebbe essere presa in considerazione nell'ambito degli appalti pubblici. Sebbene tutti i titolari abbiano il dovere di integrare la DPbDD nelle attività di trattamento, questa disposizione incentiva l'adozione dei principi di protezione dei dati nella misura in cui le pubbliche amministrazioni dovrebbero dare il buon esempio. Il titolare è tenuto ad assicurare il rispetto degli obblighi di DPbDD in relazione al trattamento svolto dai rispettivi responsabili e sub-responsabili e, pertanto, deve tenerne conto quando stipula contratti con tali soggetti.
2. Il requisito di cui all'articolo 25 obbliga i titolari a provvedere affinché la protezione dei dati sia integrata nel trattamento dei dati personali fin dalla progettazione e per impostazione predefinita durante l'intero ciclo di vita del trattamento. La DPbDD è un requisito anche per i sistemi di trattamento già esistenti all'entrata in vigore del RGPD; i titolari devono far sì che il trattamento sia aggiornato in modo coerente, in linea con il RGPD. Per maggiori informazioni su come mantenere un sistema esistente allineato alla DPbDD, cfr. il sottocapitolo 2.1.4 delle presenti linee guida. Il fulcro della disposizione è garantire una *adeguata ed efficace protezione dei dati fin dalla progettazione e una protezione per impostazione predefinita*, il che significa che i titolari dovrebbero essere in grado di dimostrare che incorporano nel trattamento le misure e le garanzie adeguate ad assicurare l'efficacia dei principi di protezione dei dati, dei diritti e delle libertà degli interessati.
3. Il capitolo 2 delle linee guida è incentrato su un'interpretazione dei requisiti previsti dall'articolo 25 ed esplora gli obblighi giuridici introdotti dalla disposizione. Il capitolo 3 fornisce esempi su come applicare la DPbDD nell'ambito di specifici principi di protezione dei dati.
4. Le linee guide esaminano l'opportunità di stabilire un meccanismo di certificazione per dimostrare la conformità con l'articolo 25 nel capitolo 4, mentre il capitolo 5 riguarda le modalità di verifica dell'attuazione dell'articolo 25 da parte delle autorità di controllo. Infine, le linee guida forniscono alle parti interessate ulteriori raccomandazioni su come attuare con successo la DPbDD. L'EDPB riconosce i problemi che le piccole e medie imprese (in prosieguo: «PMI») incontrano nel dare piena esecuzione agli obblighi della DPbDD e fornisce ulteriori raccomandazioni specifiche per le PMI nel capitolo 6.

2. ANALISI DELL'ARTICOLO 25, PARAGRAFI 1 E 2: PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

5. L'obiettivo del presente capitolo è esplorare e fornire indicazioni sui requisiti relativi rispettivamente alla protezione dei dati fin dalla progettazione di cui all'articolo 25, paragrafo 1, e alla protezione dei dati per impostazione predefinita di cui all'articolo 25, paragrafo 2. La protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita sono concetti complementari che si rafforzano vicendevolmente. Gli interessati trarranno maggiori benefici dalla protezione dei dati per impostazione predefinita se verrà attuata contestualmente la protezione dei dati fin dalla progettazione, e viceversa.
6. La DPbDD è un requisito che si applica a tutti i titolari del trattamento, dalle piccole imprese alle imprese multinazionali. Di conseguenza, la complessità dell'attuazione della DPbDD può variare a seconda dello specifico trattamento. Indipendentemente dalle dimensioni, comunque, in tutti i casi si possono conseguire vantaggi per il titolare del trattamento e per l'interessato attraverso l'attuazione della DPbDD.

2.1 ARTICOLO 25, PARAGRAFO 1: PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE

2.1.1 OBBLIGO DEL TITOLARE DEL TRATTAMENTO DI ATTUARE MISURE TECNICHE E ORGANIZZATIVE ADEGUATE E LE NECESSARIE GARANZIE NEL TRATTAMENTO

7. In linea con l'articolo 25, paragrafo 1, il titolare attua *misure* tecniche e organizzative *adeguate* che sono concepite per attuare i principi di protezione dei dati e integra nel trattamento le *necessarie garanzie* per adempiere ai requisiti e tutelare i diritti e le libertà degli interessati. Sia le misure adeguate che le necessarie garanzie intendono perseguire la medesima finalità di tutelare i diritti degli interessati e garantire che la protezione dei loro dati personali sia integrata nel trattamento.
8. Le espressioni *misure tecniche e organizzative* e necessarie garanzie possono essere intese in senso lato come qualsiasi metodo o mezzo che un titolare può impiegare nel trattamento. Con il termine adeguate si intende che le misure e le necessarie garanzie devono essere idonee a conseguire la finalità prevista, ossia devono attuare *efficacemente* i principi di protezione dei dati[3]. Il requisito di adeguatezza è quindi strettamente connesso al requisito di efficacia.
9. Per garanzia e misura tecnica od organizzativa s'intende tutto ciò che è compreso fra l'uso di soluzioni tecniche avanzate e la formazione di base del personale. Ne sono esempi idonei, a seconda del contesto e dei rischi associati al trattamento in questione, la pseudonimizzazione dei dati personali[4], la memorizzazione di dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico, la possibilità per gli interessati di intervenire nel trattamento, la fornitura di informazioni sulla conservazione

dei dati personali, la disponibilità di sistemi di rilevamento di malware, la formazione dei dipendenti sull'«igiene informatica» di base, l'istituzione di sistemi di gestione della privacy e della sicurezza delle informazioni, l'obbligo contrattuale per i responsabili del trattamento di attuare prassi specifiche di minimizzazione dei dati, ecc.

10. Standard, migliori prassi e codici di condotta riconosciuti da associazioni e da altri organismi che rappresentano categorie di titolari del trattamento possono essere utili ai fini della determinazione di misure adeguate. Tuttavia, il titolare deve verificare l'adeguatezza delle misure con riguardo allo specifico trattamento.

2.1.2 VOLTE AD ATTUARE I PRINCIPI DI PROTEZIONE DEI DATI IN MODO EFFICACE E TUTELARE I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI

11. I *principi di protezione dei dati* sono fissati all'articolo 5 (in prosieguo: «i principi»), i *diritti e le libertà degli interessati* sono i diritti e le libertà fondamentali di persone fisiche, e in particolare il loro diritto alla protezione dei dati personali, la cui tutela, a norma dell'articolo 1, paragrafo 2, è l'obiettivo del RGPD (in prosieguo «i diritti»)[5]. La loro precisa formulazione è contenuta nella Carta dei diritti fondamentali dell'UE. È essenziale che il titolare del trattamento comprenda il significato dei *principi* e dei *diritti* in quanto fondamento della protezione offerta dal RGPD e in particolare dall'obbligo della DPbDD.

12. Quando si attuano misure tecniche e organizzative adeguate, tali misure e le garanzie devono essere *concepite* in funzione dell'efficace attuazione di ognuno dei summenzionati principi e della conseguente tutela dei diritti.

Conseguire l'efficacia

13. L'efficacia è al cuore del concetto di protezione dei dati fin dalla progettazione. L'obbligo di attuare i principi in modo efficace comporta che i titolari del trattamento applichino le misure e le garanzie necessarie per la tutela di tali principi, al fine di garantire i diritti degli interessati. Ogni misura attuata deve produrre i risultati perseguiti per il trattamento e previsti dal titolare. Questa osservazione comporta due conseguenze.

14. In primo luogo, ciò significa che l'articolo 25 non richiede l'attuazione di misure tecniche e organizzative specifiche, bensì che le misure e le garanzie scelte siano specificamente connesse all'attuazione dei principi di protezione dei dati nello specifico trattamento. In tal senso, le misure e le garanzie devono essere concepite per essere robuste e il titolare del trattamento deve essere in grado di attuare ulteriori misure al fine di far fronte a un eventuale aumento dei rischi[6]. Il fatto che le misure siano o meno efficaci dipenderà quindi dal contesto del trattamento in questione e dalla valutazione di taluni elementi che devono essere presi in considerazione al momento di determinare i mezzi del trattamento. I suddetti elementi saranno trattati di seguito al sottocapitolo 2.1.3.

15. In secondo luogo, i titolari del trattamento devono essere in grado di dimostrare che i principi siano stati rispettati.

16. Le misure e le garanzie attuate devono conseguire l'effetto auspicato in termini di protezione dei dati e il titolare del trattamento deve disporre della documentazione relativa alle misure tecniche e organizzative[7]. A tale scopo, il titolare può definire idonei indicatori chiave di prestazione (ICP/KPI) per dimostrare l'efficacia. Un ICP è un valore misurabile scelto dal titolare che dimostra con quanta efficacia questi riesca a conseguire il suo obiettivo di protezione dei dati. Gli ICP possono essere *quantitativi*, come la percentuale di falsi positivi o falsi negativi, la riduzione dei reclami, la diminuzione del tempo di risposta quando gli interessati esercitano i loro diritti; o *qualitativi*, come le valutazioni di prestazione, l'uso di tabelle di classificazione o le valutazioni di esperti. In alternativa agli ICP, i titolari possono dimostrare che l'attuazione dei principi è efficace indicando i criteri alla base della loro valutazione dell'efficacia delle misure e delle garanzie scelte.

2.1.3 ELEMENTI DI CUI TENERE CONTO

17. L'articolo 25, paragrafo 1, elenca gli elementi di cui il titolare deve tenere conto allorché determina le misure riferite a un trattamento specifico. Di seguito sono fornite linee guida sull'applicazione di tali elementi nel processo di progettazione, compresa la progettazione delle impostazioni predefinite. Tutti questi elementi contribuiscono a determinare se una misura sia adeguata ai fini dell'efficace attuazione dei principi; pertanto nessuno fra essi costituisce un obiettivo da raggiungere in quanto tale, trattandosi piuttosto di fattori da considerare nel loro insieme in vista del raggiungimento dell'obiettivo perseguito.

2.1.3.1 Stato dell'arte

18. Il concetto di «stato dell'arte» è rinvenibile in diversi acquis dell'UE, ad es. in materia di tutela dell'ambiente o di sicurezza dei prodotti. Nel RGPD lo «stato dell'arte»[8] è menzionato non soltanto nell'articolo 32 in relazione alle misure di sicurezza[9] [10], ma anche nell'articolo 25, cosicché questo parametro di riferimento è applicabile a tutte le misure tecniche e organizzative integrate nel trattamento.

19. Nell'ambito dell'articolo 25, il riferimento allo «stato dell'arte» impone l'obbligo ai titolari, allorché determinano le misure tecniche e organizzative adeguate, **di tenere conto degli attuali progressi compiuti dalla tecnologia** disponibile sul mercato. Ciò comporta che i titolari debbano essere a conoscenza dei progressi tecnologici e rimanere sempre aggiornati sulle opportunità e i rischi per il trattamento, in termini di protezione dei dati, derivanti dalle tecnologie e su come mettere in atto e aggiornare le misure e le garanzie che *assicurano un'attuazione efficace* dei principi e dei diritti degli interessati tenendo conto dell'evoluzione del panorama tecnologico.

20. Lo «stato dell'arte» è un concetto dinamico che non può essere definito staticamente con riguardo a un determinato momento, bensì dovrebbe essere oggetto di una valutazione *continuativa* nel contesto dei progressi tecnologici. Di fronte a tali progressi, un titolare può riscontrare che una misura in precedenza atta a conferire un livello di protezione adeguato ora non lo è più. Trascurare l'aggiornamento sui progressi tecnologici potrebbe, quindi, comportare una mancata osservanza dell'articolo 25.
21. Il criterio dello «stato dell'arte» non si applica esclusivamente alle misure tecnologiche, ma anche a quelle organizzative. La mancanza di misure organizzative adeguate può ridurre o compromettere del tutto l'efficacia di una tecnologia scelta. Possono costituire esempi di misure organizzative l'adozione di politiche interne, la formazione aggiornata in materia di tecnologia, sicurezza e protezione dei dati nonché politiche di gestione e di *governance* della sicurezza informatica.
22. Quadri di riferimento standard, certificazioni, codici di condotta ecc. esistenti e riconosciuti possono contribuire a indicare l'attuale «stato dell'arte» nello specifico ambito di utilizzo. Qualora tali standard esistano e prevedano un livello elevato di protezione per l'interessato in conformità (o in misura superiore) ai requisiti giuridici, i titolari dovrebbero tenerne conto nella progettazione e nell'attuazione delle misure di protezione dei dati.

2.1.3.2 Costi di attuazione

23. Il titolare può tenere conto del costo di attuazione allorché sceglie e applica misure tecniche e organizzative adeguate e garanzie necessarie che mettono efficacemente in atto i principi al fine di tutelare i diritti degli interessati. Il costo si riferisce alle risorse in generale, compresi il tempo e le risorse umane.
24. Il fattore costo implica che il titolare non impieghi una quantità sproporzionata di risorse nel caso in cui esistano misure alternative, meno dispendiose, ma efficaci. Tuttavia, il costo di attuazione rappresenta un fattore di cui tenere conto nel realizzare la protezione dei dati fin dalla progettazione, e non già un motivo per astenersi dal realizzarla.
25. Le misure individuate devono pertanto garantire che l'attività di trattamento prevista dal titolare non comporti trattamenti di dati personali in violazione dei principi, indipendentemente dal costo di tali misure. I titolari devono essere in grado di gestire i costi complessivi per poter attuare efficacemente tutti i principi e, di conseguenza, tutelare i diritti.

2.1.3.3 Natura, ambito di applicazione, contesto e finalità del trattamento

26. I titolari devono tenere conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento allorché determinano le misure necessarie.
27. Questi fattori devono essere interpretati in modo coerente con il ruolo ad essi attribuito in altre disposizioni del RGPD, quali gli articoli 24, 32 e 35,

allo scopo di integrare principi di protezione dei dati nella progettazione del trattamento.

28. In breve, il concetto di **natura** può essere inteso come le caratteristiche intrinseche[11] del trattamento. L'**ambito di applicazione** fa riferimento alla dimensione e all'ampiezza del trattamento. Il **contesto** riguarda le circostanze nel trattamento che possono influenzare le aspettative degli interessati, mentre la **finalità** si riferisce agli obiettivi del trattamento.

2.1.3.4 Rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento

29. Il RGPD adotta un approccio coerente basato sul rischio in molte delle sue disposizioni, negli articoli 24, 25, 32 e 35, al fine di individuare le misure tecniche e organizzative adeguate per tutelare le persone fisiche e i loro dati personali nonché adempiere ai requisiti del RGPD. I beni da tutelare sono sempre gli stessi (le persone fisiche, mediante la protezione dei loro dati personali), identici sono i rischi (per i diritti delle persone fisiche), e identiche le condizioni di cui tenere conto (natura, ambito di applicazione, contesto e finalità del trattamento).

30. Nell'analizzare i rischi ai fini del rispetto di quanto prevede l'articolo 25, il titolare deve individuare i rischi per i diritti degli interessati associati a una violazione dei principi, e determinare la loro probabilità e gravità al fine di attuare misure efficaci di mitigazione di tali rischi. Un esame sistematico e approfondito del trattamento è fondamentale nel corso della valutazione dei rischi. Per esempio, un titolare valuta i rischi specifici associati all'assenza di un consenso liberamente espresso, assenza che rappresenta una violazione del principio di liceità, nel trattamento dei dati personali di minori in quanto gruppo vulnerabile, ove non sussista alcun altro fondamento giuridico, e attua misure adeguate per contrastare e mitigare efficacemente i rischi associati a questo gruppo di interessati.

31. Le «Linee guida in materia di valutazione d'impatto sulla protezione dei dati» dell'EDPB[12], che descrivono un approccio utile a stabilire se un trattamento possa presentare un rischio elevato o meno per l'interessato, forniscono anche indicazioni su come valutare i rischi per la protezione dei dati ed effettuarne una valutazione. Tali linee guida possono altresì risultare utili durante la valutazione dei rischi in tutti gli articoli summenzionati, compreso l'articolo 25.

32. L'approccio basato sul rischio non esclude l'utilizzo di dati di riferimento, migliori prassi e standard. Questi potrebbero fornire strumenti utili ai titolari per affrontare rischi simili in situazioni analoghe (natura, ambito di applicazione, contesto e finalità del trattamento). Tuttavia, permane l'obbligo previsto dall'articolo 25 (nonché dagli articoli 24, 32 e 35, paragrafo 7, lettera c)), di tenere conto dei *«rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento»*. Pertanto i titolari, anche ove supportati da tali strumenti, devono sempre effettuare caso per caso una

valutazione dei rischi per la protezione dei dati insiti nell'attività di trattamento corrente e verificare l'efficacia delle misure e delle garanzie adeguate proposte. Potrebbe rendersi necessario anche effettuare una valutazione d'impatto sulla protezione dei dati, ovvero aggiornare una tale valutazione ove già esistente.

2.1.4 ASPETTO TEMPORALE

2.1.4.1 Al momento di determinare i mezzi del trattamento

33. La protezione dei dati fin dalla progettazione deve essere attuata «*al momento di determinare i mezzi del trattamento*».

34. I «*mezzi del trattamento*» variano dagli elementi generali della progettazione di un trattamento fino a quelli dettagliati, e comprendono l'architettura, le procedure, i protocolli, il layout e l'aspetto.

35. Il «*momento di determinare i mezzi del trattamento*» si riferisce al periodo in cui il titolare decide come verrà effettuato il trattamento e il modo in cui si svolgerà, nonché i meccanismi che verranno impiegati per effettuarlo. È nel processo di adozione di queste decisioni che il titolare deve valutare le misure e le garanzie adeguate per attuare efficacemente i principi e i diritti degli interessati nel trattamento e considerare i rischi e gli elementi, quali lo stato dell'arte, il costo di attuazione, la natura, l'ambito di applicazione, il contesto e la finalità, ivi compreso il tempo per ottenere e poter utilizzare il software, l'hardware e i servizi per il trattamento dei dati.

36. La considerazione dei requisiti di DPbDD in fase precoce è di importanza cruciale per attuare con successo i principi e tutelare i diritti degli interessati. Inoltre, dal punto di vista del rapporto costi/benefici, è anche nell'interesse dei titolari tenere conto della DPbDD prima piuttosto che dopo, poiché potrebbe risultare difficile e costoso modificare in un momento successivo pianificazioni già definite e trattamenti già progettati.

2.1.4.2 All'atto del trattamento stesso (mantenimento e verifica dei requisiti in materia di protezione dei dati)

37. Una volta avviato il trattamento, il titolare è tenuto a mantenere su base continuativa la DPbDD, ossia a dare attuazione efficace e costante ai principi al fine di tutelare i diritti, tenendosi aggiornato sullo stato dell'arte, riesaminando il livello di rischio, ecc. La natura, l'ambito di applicazione e il contesto delle operazioni di trattamento, nonché il rischio possono mutare nel corso del trattamento, comportando per il titolare l'obbligo di verificare tali operazioni per mezzo di valutazioni e riesami periodici dell'efficacia delle misure e garanzie che ha scelto.

38. L'obbligo di mantenere, verificare e aggiornare, ove necessario, il trattamento si applica altresì ai sistemi preesistenti. Ciò implica che i sistemi progetta-

ti prima dell'entrata in vigore del RGPD devono essere sottoposti a verifiche e manutenzione per garantire l'applicazione di misure e garanzie che mettano in atto i principi e i diritti degli interessati in modo efficace, come indicato nelle presenti linee guida.

39. Tale obbligo si estende anche ai trattamenti svolti per mezzo di responsabili del trattamento. Le operazioni di trattamento effettuate dai responsabili dovrebbero essere regolarmente esaminate e valutate dai titolari per garantire che continuino a rispettare i principi e permettano ai titolari di adempiere ai rispettivi obblighi in tale contesto.

2.2 ARTICOLO 25, PARAGRAFO 2: PROTEZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA

2.2.1 Siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento

40. In ambito informatico, per «impostazione predefinita» si intende comunemente un valore preesistente o preselezionato di un'impostazione configurabile che viene assegnato a un'applicazione informatica, a un programma informatico o a una periferica. Tali impostazioni sono anche chiamate «impostazioni di fabbrica», specialmente per i dispositivi elettronici.

41. Pertanto, l'espressione «per impostazione predefinita» nell'ambito del trattamento di dati personali si riferisce alle scelte compiute rispetto a valori di configurazione od opzioni di trattamento che sono rispettivamente fissati o prescritte in un sistema di trattamento (un'applicazione informatica, un servizio o una periferica o una procedura di trattamento manuale), tali da incidere sulla quantità dei dati personali raccolti, sulla portata del trattamento, sul periodo di conservazione e sull'accessibilità.

42. Il titolare dovrebbe scegliere, assumendosene la responsabilità, opzioni e impostazioni predefinite per il trattamento tali da garantire che venga effettuato per impostazione predefinita solo il trattamento strettamente necessario per conseguire la specifica e lecita finalità. In questo caso, i titolari dovrebbero affidarsi alla loro valutazione della necessità del trattamento in relazione alle basi giuridiche di cui all'articolo 6, paragrafo 1. Ciò significa che, per impostazione predefinita, il titolare non deve raccogliere più dati del necessario, non deve trattare i dati acquisiti oltre quanto sia necessario per le sue finalità né deve conservarli per un periodo superiore a quello necessario. Il requisito di base prevede che la protezione dei dati sia integrata nel trattamento per impostazione predefinita.

43. Il titolare è tenuto a definire in anticipo per quali finalità specifiche, esplicite e legittime i dati personali vengono raccolti e trattati[13]. Le misure devono, per impostazione predefinita, essere adeguate a garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento. Le linee guida dell'EDPS per valutare la necessità e la proporzionalità delle misure che limitano il diritto alla protezione dei dati personali possono essere

utili anche per decidere quali dati sia necessario trattare per conseguire una finalità specifica[14] [15] [16].

44. Se il titolare utilizza software commerciali o di terzi, deve eseguire una valutazione dei rischi del prodotto e accertarsi che siano disattivate le funzioni che non hanno una base giuridica o non sono compatibili con le finalità previste del trattamento.

45. Le stesse considerazioni si applicano alle misure organizzative a sostegno dei trattamenti. Esse dovrebbero essere concepite, sin dall'inizio, per trattare soltanto la quantità minima di dati personali necessari per i trattamenti specifici. Ciò dovrebbe essere tenuto particolarmente in conto nello stabilire le modalità di accesso ai dati da parte di personale con ruoli ed esigenze di accesso diversi.

46. La nozione di «misure tecniche e organizzative» adeguate nel contesto della protezione dei dati per impostazione predefinita va dunque intesa nel senso già indicato al sottocapitolo 2.1.1, ma riferendola specificamente all'attuazione del principio della minimizzazione dei dati.

47. L'obbligo sopra illustrato di trattare solo i dati personali necessari per ciascuna finalità specifica si applica agli elementi indicati qui di seguito.

2.2.2 PERIMETRO DELL'OBBLIGO DI MINIMIZZAZIONE DEI DATI

48. L'articolo 25, paragrafo 2, indica il perimetro dell'obbligo di minimizzazione dei dati, affermando che tale obbligo vale per la quantità di dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità dei dati.

2.2.2.1 Quantità dei dati personali raccolti

49. I titolari dovrebbero tenere conto sia del volume dei dati personali sia delle tipologie, delle categorie e del livello di dettaglio dei dati personali richiesti per le finalità del trattamento. Le loro scelte nella progettazione dovrebbero tenere conto dei maggiori rischi per i principi di integrità e riservatezza, di minimizzazione dei dati e della limitazione della conservazione connessi alla raccolta di grandi quantità di dati personali dettagliati, rispetto ai minori rischi associati alla raccolta di quantità minori di dati e/o di informazioni meno dettagliate sugli interessati. In ogni caso, le impostazioni predefinite non devono includere la raccolta di dati personali che non sono necessari per la specifica finalità del trattamento. In altre parole, se determinate categorie di dati personali sono superflue o se non sono necessari dati particolareggiati, perché sono sufficienti dati meno granulari, allora quelli in eccesso non sono raccolti.

50. Gli stessi requisiti di base valgono per i servizi indipendentemente dalla piattaforma o dal dispositivo in uso; è possibile raccogliere solo i dati personali necessari per la finalità considerata.

2.2.2.2 La portata del trattamento

51. I trattamenti[17] effettuati sui dati personali devono limitarsi a quanto è necessario. Molte operazioni di trattamento possono contribuire a realizzare la finalità perseguita dallo specifico trattamento. Nondimeno, il fatto che taluni dati personali siano necessari per conseguire una determinata finalità non significa che sia possibile sottoporre a trattamento tutte le tipologie di tali dati e con qualsiasi frequenza. I titolari dovrebbero inoltre fare attenzione a non ampliare i limiti delle «finalità compatibili» di cui all'articolo 6, paragrafo 4, e avere presente quali trattamenti possano corrispondere alle ragionevoli aspettative degli interessati.

2.2.2.3 Il periodo di conservazione

52. I dati personali raccolti non devono essere conservati se non sono necessari per la finalità del trattamento e non sussiste altra finalità compatibile né altro fondamento giuridico ai sensi dell'articolo 6, paragrafo 4. Qualsiasi conservazione dovrebbe essere obiettivamente giustificabile da parte del titolare del trattamento in quanto necessaria, in base al principio di responsabilizzazione.
53. Il titolare del trattamento deve limitare il periodo di conservazione all'arco di tempo necessario per il raggiungimento della specifica finalità. Se i dati personali non sono più necessari ai fini del trattamento, allora per impostazione predefinita sono cancellati o resi anonimi. La durata del periodo di conservazione dipenderà pertanto dalla finalità del trattamento in questione. Questo obbligo è direttamente correlato al principio di limitazione della conservazione di cui all'articolo 5, paragrafo 1, lettera e), e viene attuato per impostazione predefinita, ossia il titolare dovrebbe disporre di procedure sistematiche per la cancellazione o l'anonimizzazione dei dati, integrate nel trattamento.
54. L'anonimizzazione[18] dei dati personali costituisce un'alternativa alla cancellazione, a condizione che siano presi in considerazione tutti gli elementi contestuali pertinenti e che siano regolarmente valutate la probabilità e la gravità del rischio, compreso il rischio di re-identificazione[19].

2.2.2.4 Accessibilità dei dati

55. Il titolare dovrebbe prevedere limitazioni quanto ai soggetti abilitati all'accesso e alla tipologia dell'accesso ai dati personali sulla base di una valutazione della necessità e assicurare che i dati personali siano realmente accessibili a chi ne ha bisogno in caso di necessità, ad esempio in situazioni critiche. I controlli dell'accesso dovrebbero essere effettuati per l'intero flusso di dati durante il trattamento.
56. L'articolo 25, paragrafo 2, stabilisce peraltro che non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento

della persona fisica. Il titolare deve limitare l'accessibilità, per impostazione predefinita, e dare all'interessato la possibilità di intervenire prima di pubblicare o altrimenti rendere disponibili i suoi dati personali a un numero indefinito di persone fisiche.

57. Rendere disponibili i dati personali a un numero indefinito di persone potrebbe comportare una divulgazione dei dati ancora più ampia rispetto a quella inizialmente prevista, il che è particolarmente pertinente nel contesto di Internet e dei motori di ricerca; perciò i titolari dovrebbero, per impostazione predefinita, dare agli interessati l'opportunità di intervenire prima che i dati personali vengano messi a disposizione pubblicamente su Internet. Questo aspetto è particolarmente importante nel caso di minori e gruppi vulnerabili.

58. A seconda della base giuridica del trattamento, le modalità di intervento potrebbero variare in rapporto al contesto del trattamento (per esempio può essere necessario richiedere il consenso per la diffusione di dati personali o prevedere impostazioni di privacy affinché gli interessati stessi possano controllare l'accesso del pubblico).

59. Anche nell'ipotesi in cui i dati personali siano diffusi con il permesso e la consapevolezza di un interessato, ciò non significa che ogni altro titolare in grado di accedere ai dati personali possa trattarli liberamente per le proprie finalità; questi deve infatti disporre di una specifica base giuridica [20].

3. ATTUAZIONE DEI PRINCIPI DI PROTEZIONE NEL TRATTAMENTO DEI DATI PERSONALI UTILIZZANDO LA PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E LA PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

60. In tutte le fasi della progettazione delle attività di trattamento, compresi gli appalti, le gare di appalto, l'esternalizzazione, lo sviluppo, il supporto, la manutenzione, il collaudo, la conservazione, la cancellazione ecc., il titolare dovrebbe tenere conto e considerare i vari elementi della DPbDD, illustrati con esempi riportati in questo capitolo nel contesto dell'attuazione dei principi[21] [22] [23].

61. I titolari devono applicare i principi per attuare la DPbDD; tali principi, che includono la trasparenza, la liceità, la correttezza, la limitazione delle finalità, la minimizzazione dei dati, l'esattezza, la limitazione della conservazione, l'integrità, la riservatezza e la responsabilizzazione, sono indicati nell'articolo 5 e nel considerando 39 del RGPD. Per avere una conoscenza approfondita delle modalità di attuazione della DPbDD, si sottolinea l'importanza di comprendere il significato di ciascuno di questi principi.

62. Nella presentazione degli esempi su come rendere operativa la DPbDD, sono stati stilati elenchi degli **elementi chiave della DPbDD** per ciascuno dei principi. Gli esempi, pur sottolineando lo specifico principio di protezione dei dati in questione, possono sovrapporsi anche con altri principi strettamente connessi. L'EDPB evidenzia che gli elementi fondamentali e gli esempi presentati di seguito non sono né esaustivi né vincolanti, ma sono da in-

tendersi come elementi di guida per ciascuno dei principi. I titolari devono valutare come garantire la conformità ai principi nel contesto del concreto trattamento in questione.

63. Benché questa sezione tratti nello specifico l'attuazione dei principi, il titolare dovrebbe altresì mettere in atto soluzioni *appropriate* ed *efficaci* per tutelare i diritti degli interessati, anche ai sensi del capo III del RGPD, ove ciò non sia già prescritto dai principi stessi.

64. Il principio di responsabilizzazione ha natura trasversale: prevede che il titolare risponda della scelta delle misure tecniche e organizzative necessarie.

3.1 TRASPARENZA[24]

65. Il titolare deve essere chiaro e trasparente con l'interessato su come raccoglierà, utilizzerà e condividerà i dati personali. Trasparenza significa consentire agli interessati di comprendere e, se necessario, avvalersi dei loro diritti come fissati negli articoli da 15 a 22. Il principio trova fondamento negli articoli 12, 13, 14 e 34. Le misure e le garanzie tese a sostenere il principio di trasparenza dovrebbero anche concorrere all'attuazione di questi articoli.

66. Gli elementi chiave della progettazione e dell'impostazione predefinita per quanto riguarda il principio della trasparenza possono includere:

- chiarezza – le informazioni sono fornite in un linguaggio chiaro e semplice, conciso e comprensibile;
- semantica – la comunicazione deve avere un significato chiaro per il pubblico a cui è rivolta;
- accessibilità – le informazioni sono facilmente accessibili per l'interessato;
- contestualità – le informazioni devono essere fornite al momento opportuno e nella forma adeguata;
- pertinenza – le informazioni devono essere pertinenti e applicabili all'interessato specifico;
- progettazione universale – le informazioni sono accessibili a tutti gli interessati, compreso l'utilizzo di linguaggi leggibili da una macchina per agevolare e automatizzare la leggibilità e la chiarezza;
- comprensibilità – gli interessati devono avere una buona comprensione di ciò che possono aspettarsi dal trattamento dei loro dati personali, in particolare quando si tratti di minori o di soggetti appartenenti ad altre categorie vulnerabili;
- multicanalità – le informazioni dovrebbero essere fornite attraverso canali e mezzi di comunicazione diversi, non solo quelli testuali, per aumentare la probabilità che raggiungano efficacemente l'interessato;
- approccio multilivello – le informazioni devono essere fornite secondo un approccio multilivello, in modo da garantire un equilibrio tra completezza e comprensibilità, rispecchiando le ragionevoli aspettative degli interessati.

Esempio[25]

Un titolare sta progettando una politica sulla privacy sul proprio sito web per conformarsi agli obblighi di trasparenza. La politica sulla privacy non deve contenere una quantità eccessiva di informazioni di difficile comprensione per l'interessato medio, deve essere scritta in un linguaggio chiaro e conciso e consentire all'utente del sito di comprendere le modalità di trattamento dei suoi dati personali. Il titolare fornisce pertanto informazioni secondo un approccio multilivello, evidenziando i punti più importanti. Vengono rese facilmente accessibili informazioni più dettagliate e sono messi a disposizione menu a discesa e collegamenti ad altre pagine per spiegare ulteriormente i vari punti e i concetti contenuti nella politica. Il titolare fa anche in modo che le informazioni siano fornite con più canali, prevedendo video che illustrano i punti più importanti delle informazioni in forma testuale. La sinergia tra le varie pagine è fondamentale per garantire che l'approccio multilivello non aumenti la confusione anziché ridurla.

La politica sulla privacy non deve essere di difficile accesso per gli interessati. Pertanto, viene messa a disposizione ed è visibile su tutte le pagine del sito in questione di modo che l'interessato acceda sempre alle informazioni con un semplice clic. Le informazioni fornite sono altresì concepite in conformità con le migliori prassi e standard di progettazione universale per renderle accessibili a tutti.

Inoltre, le informazioni necessarie dovrebbero essere messe a disposizione nel giusto contesto e al momento adeguato. Poiché il titolare svolge molte operazioni di trattamento impiegando i dati raccolti sul sito, non è sufficiente che pubblichi una politica generale sulla privacy soltanto sul sito per conformarsi agli obblighi di trasparenza. Il titolare progetta quindi un flusso di informazioni che fornisce all'interessato le informazioni pertinenti nei contesti adeguati utilizzando ad es. snippet informativi o pop up. Ad esempio, quando si chiede all'interessato di accedere ai suoi dati personali, il titolare lo informa sulle modalità del trattamento spiegando perché tali dati siano necessari per quest'ultimo.

3.2 LICEITÀ

67. Il titolare deve identificare una base giuridica valida per il trattamento dei dati personali. Le misure e le garanzie dovrebbero concorrere all'obbligo di assicurare che l'intero ciclo di vita del trattamento sia in linea con la pertinente base giuridica.

68. Tra gli elementi principali della progettazione e dell'impostazione predefinita ai fini della liceità possono figurare:

- pertinenza –al trattamento è applicata la corretta base giuridica;
- differenziazione[26] – occorre differenziare la base giuridica utilizzata per ciascuna attività di trattamento;

- finalità specifica – la corretta base giuridica deve essere chiaramente connessa alla specifica finalità di trattamento[27];
- necessità – il trattamento deve essere necessario e non soggetto a condizioni affinché la sua finalità sia lecita;
- autonomia – all'interessato dovrebbe essere garantito il massimo grado possibile di autonomia in relazione al controllo dei propri dati personali nel quadro della base giuridica;
- ottenimento del consenso – il consenso deve essere liberamente espresso, specifico, informato e inequivocabile[28]. Occorre considerare in particolare la capacità dei minori di fornire un consenso informato;
- revoca del consenso – se il consenso è la base giuridica, il trattamento dovrebbe agevolarne la revoca. La revoca del consenso deve essere altrettanto facile quanto la sua prestazione. In caso contrario, il meccanismo del consenso attuato dal titolare non è conforme al RGPD[29];
- bilanciamento degli interessi – se la base giuridica è costituita da interessi legittimi, il titolare deve effettuare un bilanciamento ponderato, considerando in particolare lo squilibrio tra i rapporti di forza, specificamente nel caso di minori e altri gruppi vulnerabili. Devono essere previste misure e garanzie per attenuare l'impatto negativo sugli interessati;
- predeterminazione – la base giuridica è stabilita prima che il trattamento abbia luogo;
- cessazione – se la base giuridica non è più valida, il trattamento cessa di conseguenza;
- adeguamento – se vi è una modifica valida della base giuridica per il trattamento, quest'ultimo deve essere adeguato in base alla nuova base giuridica[30];
- attribuzione di responsabilità – ogniqualvolta sia prevista la contitolarità del trattamento, le parti devono suddividersi in modo chiaro e trasparente le rispettive responsabilità nei confronti dell'interessato ed elaborare le misure del trattamento conformemente a tale attribuzione di responsabilità.

Esempio

Una banca intende offrire un servizio per migliorare l'efficienza nella gestione delle richieste di mutuo. L'idea alla base del servizio è che la banca può recuperare i dati sul cliente direttamente dalle amministrazioni tributarie, previa autorizzazione di queste ultime. Questo esempio non tiene conto del trattamento di dati personali provenienti da altre fonti.

Ottenere dati personali sulla situazione finanziaria dell'interessato è necessario per espletare formalità su richiesta dell'interessato prima di sottoscrivere un contratto di mutuo[31]. Tuttavia, raccogliere dati personali direttamente dall'amministrazione tributaria non è considerato necessario, perché il cliente può sottoscrivere un contratto fornendo per proprio conto le informazioni provenienti dall'amministrazione tributaria. Anche se la banca potrebbe avere un interesse legittimo ad acquisire la dcumentazione direttamente presso le competenti autorità, ad esempio per

garantire un'efficace elaborazione della richiesta di mutuo, fornire alle banche l'accesso diretto ai dati personali dei richiedenti comporta un rischio connesso all'uso o al potenziale abuso dei diritti di accesso.

Nell'attuazione del principio di liceità, il titolare comprende che, in questo contesto, non può utilizzare il criterio della «necessità a fini contrattuali» per la parte del trattamento che prevede la raccolta dei dati personali direttamente dalle amministrazioni tributarie. Il fatto che questo specifico trattamento presenti un rischio, che vede l'interessato assumere un ruolo meno attivo nel trattamento dei propri dati, è un fattore rilevante nella valutazione della liceità del trattamento stesso. La banca conclude che questa parte del trattamento deve fondarsi su un'altra base giuridica pertinente. Nello Stato membro in cui ha sede il titolare del trattamento la normativa in vigore permette alla banca di raccogliere informazioni direttamente presso le autorità tributarie, ove l'interessato vi abbia previamente acconsentito.

La banca presenta quindi le informazioni relative al trattamento sulla piattaforma per la richiesta online in modo tale da consentire agli interessati di comprendere facilmente quali trattamenti siano necessitati e quali siano opzionali. Le opzioni di trattamento, per impostazione predefinita, non consentono di ricavare i dati direttamente da altri fonti se non dall'interessato, e l'opzione per la raccolta diretta delle informazioni è presentata in modo tale da non dissuadere l'interessato dall'astenersi. Qualsiasi consenso fornito per la raccolta dei dati direttamente presso altri titolari rappresenta un diritto di accesso temporaneo a un insieme specifico di informazioni.

Ogni consenso fornito è trattato elettronicamente in modo documentabile e gli interessati dispongono di un meccanismo di facile utilizzo per controllare ciò a cui hanno dato il consenso e revocare tale consenso.

Il titolare ha valutato preventivamente tali requisiti della DPbDD e include tutti questi criteri nelle specifiche del capitolato per l'appalto di fornitura della piattaforma. Il titolare comprende che se non include i requisiti del la piattaforma. Il titolare comprende che se non include i requisiti della DPbDD nel capitolato d'appalto, potrebbe essere troppo tardi o troppo costoso attuare la protezione dei dati successivamente.

3.3 CORRETTEZZA

69. La correttezza è un principio di natura trasversale secondo cui i dati personali non devono essere trattati in modo ingiustificatamente dannoso, illegittimamente discriminatorio, imprevisto o fuorviante per l'interessato. Le misure e le garanzie che attuano il principio della correttezza supportano anche i diritti e le libertà degli interessati, in particolare il diritto all'informazione (trasparenza), il diritto di intervenire nel trattamento (accesso, cancellazione, portabilità dei dati, rettificazione) e il diritto di limitazione del trattamen-

to (il diritto a non essere sottoposto a un processo decisionale automatizzato e non subire discriminazioni nel contesto di tali processi).

70. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi alla correttezza, possono figurare:

- autonomia – agli interessati dovrebbe essere garantito il massimo grado possibile di autonomia nel determinare l'utilizzo cui sono sottoposti i loro dati personali, nonché l'ambito di applicazione e le condizioni di tale utilizzo o trattamento;
- interazione – gli interessati devono essere in grado di comunicare ed esercitare i propri diritti in relazione ai dati personali trattati dal titolare;
- aspettativa – il trattamento dovrebbe corrispondere alle aspettative ragionevoli degli interessati;
- nessuna discriminazione – il titolare non discrimina ingiustamente gli interessati;
- nessuno sfruttamento – il titolare non deve sfruttare le esigenze o le vulnerabilità degli interessati;
- libertà di scelta – il titolare non dovrebbe «catturare» (lock-in) i propri utenti in modo scorretto. Qualora un servizio che prevede il trattamento di dati personali abbia natura proprietaria, gli utenti potrebbero essere "catturati" rispetto a tale servizio, il che può essere scorretto qualora pregiudichi la possibilità per gli interessati di esercitare il diritto alla portabilità dei dati ai sensi dell'articolo 20;
- equilibrio dei rapporti di forza - tale equilibrio dovrebbe essere un obiettivo chiave della relazione tra titolare e interessato. Occorre evitare gli squilibri nei rapporti di forza e, qualora ciò non sia possibile, è necessario individuarli e tenerne conto al fine di adottare adeguate contromisure;
- assenza di trasferimento di rischi – i titolari non dovrebbero trasferire i rischi di impresa agli interessati;
- assenza di prassi ingannevoli – le informazioni e le opzioni relative al trattamento dei dati devono essere fornite in modo obiettivo e neutrale, evitando formulazioni o meccanismi ingannevoli o manipolatori;
- rispetto dei diritti – il titolare deve rispettare i diritti fondamentali degli interessati e attuare misure e garanzie adeguate, senza comprimere tali diritti se non ove ciò sia espressamente giustificato dalla legge;
- eticità – il titolare dovrebbe guardare all'impatto complessivo del trattamento sui diritti e sulla dignità delle persone;
- veridicità – il titolare deve dichiarare le proprie modalità di trattamento dei dati personali e deve agire secondo quanto dichiarato in merito, senza fuorviare gli interessati;
- intervento umano – il titolare deve integrare un intervento umano qualificato in grado di individuare le distorsioni (bias) che le macchine possono generare, conformemente al diritto di non essere sottoposto a un processo decisionale automatizzato di cui all'articolo 22[32];
- imparzialità degli algoritmi – valutare periodicamente se gli algoritmi fun-

zionino in linea con le finalità e adeguarli per attenuare le distorsioni individuate e garantire l'imparzialità del trattamento. Gli interessati dovrebbero essere informati in merito al trattamento dei dati personali attraverso algoritmi che ne facciano oggetto di analisi o previsioni, per esempio riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti[33].

Esempio 1

Un titolare gestisce un motore di ricerca che tratta per lo più dati personali generati dagli utenti. Il titolare trae beneficio dall'avere grandi quantità di dati personali e dal poterli usare per offrire pubblicità mirata; pertanto, intende esercitare un'influenza sugli interessati per rendere possibile una raccolta e un utilizzo più ampi dei loro dati personali. Il consenso sarà raccolto presentando all'interessato diverse opzioni di trattamento.

Nell'attuazione del principio della correttezza, tenendo conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, il titolare comprende che non può presentare le opzioni in modo da indurre l'interessato a consentirgli di raccogliere più dati personali di quanto avverrebbe se le opzioni fossero presentate in modo corretto e neutrale. Ciò significa che il titolare non può presentare le opzioni di trattamento in modo tale da rendere difficile per gli interessati astenersi dalla condivisione dei propri dati ovvero modificare le proprie impostazioni di privacy e limitare il trattamento. Questi sono esempi di *dark pattern* (modelli oscuri) contrari allo spirito dell'articolo 25. Le opzioni predefinite per il trattamento non devono essere invasive e la scelta di consentire un ulteriore trattamento dovrebbe essere presentata in modo da non esercitare pressione sull'interessato affinché presti il suo consenso. Pertanto, il titolare presenta con identica visibilità le opzioni connesse alla prestazione ovvero al rifiuto del consenso, descrivendo accuratamente le conseguenze per l'interessato nei rispettivi casi.

Esempio 2

Un altro titolare tratta dati personali per fornire un servizio di streaming, in cui gli utenti possono scegliere tra il normale abbonamento di qualità standard e l'abbonamento premium di qualità più elevata. Come parte dell'abbonamento premium è prevista la prioritizzazione del servizio clienti.

Con riguardo al principio della correttezza, questo servizio prioritario concesso agli abbonati premium non può dar luogo a discriminazioni nei confronti dei normali abbonati in relazione all'esercizio dei loro diritti ai sensi dell'articolo 12 del RGPD. Ciò significa che, sebbene gli abbonati premium ricevano un servizio prioritario, tale priorità non può comportare l'assenza di misure adeguate a rispondere alle richieste dei normali abbonati senza indebito ritardo, e in ogni caso entro un mese dalla ricezione.

I clienti premium possono pagare per ricevere un servizio migliore, ma tutti

gli interessati devono godere di condizioni identiche e non discriminatorie ai fini dell'esercizio dei diritti e delle libertà di cui all'articolo 12.

3.4 LIMITAZIONE DELLE FINALITÀ[34]

71. Il titolare deve raccogliere dati per finalità specifiche, esplicite e legittime e non trattarli ulteriormente in modo incompatibile con le finalità per le quali sono stati raccolti[35]. La progettazione del trattamento dovrebbe pertanto essere definita da quanto necessario per conseguire le finalità. In caso di trattamento ulteriore, il titolare deve prima assicurarsi che tale trattamento abbia finalità compatibili con quelle originarie e progettarlo di conseguenza. La compatibilità o meno della nuova finalità è valutata in base ai criteri di cui all'articolo 6, paragrafo 4.

72. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi alla limitazione delle finalità, possono figurare:

- predeterminazione – le finalità legittime sono determinate prima della progettazione del trattamento;
- specificità – le finalità sono specificate ed esplicite in merito al motivo per cui i dati personali vengono trattati;
- orientamento in base alla finalità – la finalità del trattamento dovrebbe orientare la progettazione del trattamento e determinarne i limiti;
- necessità – la finalità determina quali sono i dati personali necessari per il trattamento;
- compatibilità – qualsiasi nuova finalità deve essere compatibile con la finalità originaria per la quale sono stati raccolti i dati e orientare le modifiche rilevanti nella progettazione;
- limitazione di trattamenti ulteriori – il titolare non dovrebbe collegare set di dati o effettuare ulteriori trattamenti per finalità diverse che sono incompatibili;
- limitazioni del riutilizzo – il titolare dovrebbe adottare misure tecniche, tra cui l'hashing e la cifratura, per limitare la possibilità di riutilizzare i dati personali. Il titolare dovrebbe inoltre prevedere misure organizzative, quali politiche e obblighi contrattuali, che limitino il riutilizzo di dati personali;
- riesame periodico – il titolare dovrebbe verificare periodicamente se il trattamento sia necessario per le finalità per le quali sono stati raccolti i dati e testare la progettazione di tale trattamento con riguardo al principio di limitazione delle finalità.

Esempio

Il titolare tratta i dati personali dei suoi clienti. La finalità del trattamento è l'esecuzione del contratto, ossia poter fornire i beni all'indirizzo corretto e ottenere il pagamento. I dati personali conservati sono lo storico degli acquisti, il nome, l'indirizzo fisico, l'indirizzo di posta elettronica e il nu-

mero di telefono.

Il titolare sta valutando l'acquisto di un prodotto per la gestione dei rapporti con la clientela che consolida tutti i dati sui clienti relativi alle vendite, al marketing e all'assistenza alla clientela. Il prodotto consente di conservare tutte le chiamate, le attività, i documenti, le e-mail e le campagne di marketing per avere una panoramica a 360 gradi del singolo cliente. Inoltre, esso è in grado di analizzare automaticamente il potere di acquisto dei clienti utilizzando le informazioni pubbliche. La finalità dell'analisi è consentire un migliore orientamento delle attività promozionali, che non rientrano nell'originaria finalità legittima del trattamento.

Per conformarsi al principio della limitazione delle finalità, il titolare impone al fornitore del prodotto di mappare le diverse attività di trattamento che utilizzano i dati personali per le finalità che gli interessano.

Dopo aver ricevuto i risultati della mappatura, il titolare valuta se la nuova finalità di marketing e quella di pubblicità mirata siano compatibili con le finalità originarie definite in fase di acquisizione dei dati e se esista una base giuridica sufficiente per il relativo trattamento. Se l'esito della valutazione non è positivo, il titolare non procederà all'utilizzo delle rispettive funzionalità. In alternativa, il titolare potrebbe scegliere di non effettuare la valutazione e rinunciare semplicemente ad avvalersi delle funzionalità del prodotto descritte.

3.5 MINIMIZZAZIONE DEI DATI

73. Solo i dati personali che sono adeguati, pertinenti e limitati a quanto **necessario** per la finalità sono sottoposti a trattamento[36]. Di conseguenza, il titolare deve predeterminare quali caratteristiche e parametri dei sistemi di trattamento nonché quali funzioni di supporto siano consentiti. La minimizzazione dei dati realizza e rende operativo il principio di necessità. Nel proseguire il trattamento, il titolare dovrebbe valutare periodicamente se i dati personali trattati siano ancora adeguati, pertinenti e necessari o se occorra cancellarli o renderli anonimi.

74. I titolari dovrebbero, in primo luogo, valutare se abbiano bisogno o meno di trattare i dati personali per le finalità che interessano loro. Il titolare dovrebbe verificare se sia possibile conseguire le finalità pertinenti trattando una quantità inferiore di dati personali o disponendo di dati personali meno dettagliati o aggregati, oppure senza doverli trattare affatto[37]. Questa verifica dovrebbe essere eseguita prima di qualunque trattamento, ma potrebbe anche aver luogo in qualsiasi momento nel corso del ciclo di vita del trattamento. Ciò è altresì conforme con l'articolo 11.

75. La minimizzazione può anche riferirsi al grado di identificazione. Se la finalità del trattamento non richiede che i set di dati definitivi si riferiscano a una persona fisica identificata o identificabile (come nelle statistiche), ma lo richiede il trattamento iniziale (ad es. prima dell'aggregazione dei dati),

il titolare cancella o rende anonimi i dati personali non appena non sia più necessaria l'identificazione. Oppure, se l'identificazione continua a essere necessaria per le altre attività di trattamento, i dati personali dovrebbero essere pseudonimizzati al fine di ridurre i rischi per i diritti degli interessati.

76. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi alla minimizzazione dei dati, possono figurare:

- evitare il trattamento dei dati – evitare del tutto il trattamento dei dati personali quando ciò sia possibile per la finalità pertinente;
- limitazione – la quantità di dati personali raccolti va limitata a ciò che è necessario per la specifica finalità;
- limitazione dell'accesso – definire il trattamento dei dati in modo tale che un numero minimo di persone abbia bisogno di accedere ai dati personali per esercitare le proprie funzioni, e limitare l'accesso di conseguenza;
- pertinenza – i dati personali devono essere pertinenti al trattamento in questione e il titolare deve essere in grado di dimostrare tale pertinenza;
- necessità – ogni categoria di dati personali deve essere necessaria per le finalità specificate e dovrebbe essere trattata soltanto se non è possibile conseguire la specifica finalità con altri mezzi;
- aggregazione – quando possibile, utilizzare dati aggregati;
- pseudonimizzazione – pseudonimizzare i dati personali quando non è più necessario disporre di dati personali identificabili e memorizzare le chiavi di identificazione separatamente;
- anonimizzazione e cancellazione – se i dati personali non sono necessari per la specifica finalità (o non lo sono più), devono essere resi anonimi o cancellati;
- flusso dei dati – il flusso dei dati deve essere efficiente così da non creare copie ulteriori rispetto a quanto necessario;
- «stato dell'arte» – il titolare dovrebbe applicare tecnologie aggiornate e adeguate per evitare o minimizzare il trattamento dei dati.

Esempio 1

Una libreria intende aumentare le entrate vendendo i libri online. Il proprietario vuole creare un modello standardizzato per il procedimento di ordinazione. Per garantire che i clienti forniscano tutte le informazioni richieste, il proprietario della libreria rende obbligatori tutti i campi del modulo (se non si compilano tutti i campi il cliente non può effettuare l'ordine). Inizialmente, il proprietario del negozio online usa un modulo di contatto standard in cui si chiedono al cliente informazioni quali la data di nascita, il numero di telefono e l'indirizzo di casa. Tuttavia, i campi del modulo non sono tutti necessari per l'acquisto e la spedizione dei libri. In questo caso specifico, se l'interessato paga il prodotto in anticipo, la sua data di nascita e il suo numero di telefono non sono necessari per l'acquisto. Ciò significa che questi campi del modulo web non devono essere necessariamente compilati per ordinare il prodotto, a meno che il titolare possa dimo-

strare chiaramente che la loro compilazione è altrimenti indispensabile, e per quali motivi. Inoltre, vi sono situazioni in cui l'indirizzo non è necessario. Per esempio, quando si ordina un e-book, il cliente può scaricare il prodotto direttamente sul proprio dispositivo.

Il proprietario decide quindi di creare due moduli web: uno per ordinare i libri con un campo contenente l'indirizzo del cliente e un altro per ordinare gli e-book senza il campo dell'indirizzo.

Esempio 2

Un'azienda di trasporto pubblico intende raccogliere informazioni statistiche basate sui tragitti dei viaggiatori che consentano di operare scelte adeguate sulle modifiche degli orari del trasporto pubblico e sugli itinerari dei treni. I passeggeri devono passare il loro biglietto attraverso un lettore ogni volta che salgono o scendono da un mezzo di trasporto. Sulla base di una valutazione dei rischi per i diritti e le libertà dei passeggeri legati alla raccolta dei loro itinerari di viaggio, il titolare stabilisce che è possibile identificare i passeggeri ove questi risiedano o lavorino in aree scarsamente popolate attraverso l'identificazione del singolo itinerario, desumibile grazie all'identificativo del biglietto. Poiché tale identificativo non è necessario per ottimizzare gli orari del trasporto pubblico e gli itinerari dei treni, il titolare non lo conserva. Una volta terminato il tragitto, il titolare conserva solo i singoli itinerari di viaggio in modo da non poter identificare i tragitti collegati a uno specifico biglietto, memorizzando soltanto le informazioni sui singoli percorsi di viaggio.

Qualora si manifesti comunque il rischio di identificare una persona esclusivamente a partire dal suo itinerario di viaggio , il titolare attua misure statistiche per ridurre tale rischio, per esempio eliminando le informazioni sul luogo di partenza e di destinazione.

Esempio 3

Un corriere intende valutare l'efficacia delle sue consegne in termini di tempistiche, programmazione del lavoro e consumo di carburante. Per raggiungere questo obiettivo, il corriere deve trattare una serie di dati personali relativi sia ai dipendenti (conducenti) sia ai clienti (indirizzi, articoli da spedire, ecc.). Questo trattamento comporta rischi sia in termini di sorveglianza dei dipendenti, per i quali occorrono specifiche salvaguardie di natura giuridica, sia in termini di rilevamento delle abitudini dei clienti attraverso la conoscenza dei prodotti consegnati nel tempo. Tali rischi possono essere significativamente ridotti tramite una pseudonimizzazione adeguata dei dati relativi a dipendenti e clienti. In particolare, con una rotazione frequente dei codici di pseudonimizzazione e focalizzandosi su macro-aree anziché sui singoli indirizzi, si realizza un'efficace minimizzazione

dei dati e il titolare può concentrarsi esclusivamente sul processo di spedizione e sulla finalità di ottimizzazione delle risorse senza sconfinare nel monitoraggio dei comportamenti dei singoli (clienti o dipendenti).

Esempio 4

Un ospedale sta acquisendo dati sui pazienti nell'ambito di un sistema informativo ospedaliero (cartelle cliniche elettroniche). Il personale ospedaliero ha bisogno di accedere ai fascicoli dei pazienti per poter adottare decisioni informate in merito alla loro assistenza e alle cure, nonché al fine di documentare tutte le attività effettuate in materia di diagnosi, assistenza e cura. Per impostazione predefinita, l'accesso è consentito solo ai membri del personale medico cui sia affidata la cura del rispettivo paziente nel reparto specifico cui questi è stato assegnato. Il gruppo di persone che ha accesso al fascicolo di un paziente viene ampliato se nella cura sono coinvolti altri reparti o unità diagnostiche. Una volta dimesso il paziente e completata la fatturazione, l'accesso è limitato a un piccolo gruppo di dipendenti, per ciascun reparto specifico, che risponde alle richieste di informazioni mediche o di consultazione effettuate da altri fornitori di servizi medici, previa autorizzazione del paziente in questione.

3.6 ESATTEZZA

77. I dati personali devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati[38].

78. I requisiti dovrebbero essere esaminati in relazione ai rischi e alle conseguenze derivanti dall'utilizzo concreto dei dati. I dati inesatti potrebbero costituire un rischio per i diritti e le libertà degli interessati, ad esempio quando conducono a una diagnosi errata o a un trattamento errato di un protocollo sanitario, oppure un'immagine errata di una persona può portare a decisioni erronee sia attraverso processi manuali sia attraverso un processo decisionale automatizzato o l'impiego di tecniche di intelligenza artificiale.

79. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi all'esattezza, possono figurare:

- fonte dei dati – le fonti dei dati personali dovrebbero essere affidabili in termini di esattezza dei dati;
- grado di esattezza – ciascun elemento dei dati personali deve essere il più esatto possibile in base alle necessità delle finalità specifiche;
- esattezza misurabile – occorre ridurre il numero di falsi positivi/negativi, per esempio le distorsioni generate nell'ambito delle decisioni automatizzate e dell'intelligenza artificiale;
- verifica – a seconda della natura dei dati, e in relazione alla frequenza delle

relative modifiche, il titolare dovrebbe verificare la correttezza dei dati personali presso l'interessato prima del trattamento e nelle sue diverse fasi (per esempio rispetto ai requisiti di età);

- cancellazione/rettifica – il titolare dovrebbe cancellare o rettificare tempestivamente i dati inesatti e, in particolare, agevolare questa procedura se gli interessati sono o erano minori e successivamente desiderano eliminare i suddetti dati personali[39];
- evitare la propagazione di errori – i titolari dovrebbero attenuare l'effetto di un errore accumulato nella catena di trattamento;
- accesso – gli interessati dovrebbero ricevere informazioni sui dati personali e disporre di un accesso efficace agli stessi, ai sensi degli articoli da 12 a 15 del RGPD, per controllarne l'esattezza e apportare le rettifiche ove necessario;
- esattezza permanente – i dati personali dovrebbero essere esatti in tutte le fasi del trattamento e nelle fasi critiche dovrebbero essere effettuate verifiche di esattezza;
- aggiornamento – i dati personali sono aggiornati qualora ciò sia necessario per la specifica finalità;
- progettazione dei dati – impiego di caratteristiche organizzative e tecnologiche di progettazione per ridurre le eventuali inesattezze, per esempio proponendo scelte concise e predeterminate anziché campi a testo libero.

Esempio 1

Una compagnia assicurativa desidera servirsi dell'intelligenza artificiale (IA) per eseguire la profilazione dei clienti che acquistano le polizze, utilizzandola quale fondamento del suo processo decisionale in fase di calcolo del rischio assicurativo. Nel determinare come sviluppare tali soluzioni di IA, la compagnia stabilisce i mezzi del trattamento: in tale contesto dovrebbe considerare la protezione dei dati fin dalla progettazione al momento di scegliere un'applicazione di IA da un fornitore e decidere come utilizzarla. Nello stabilire come utilizzare l'IA, il titolare dovrebbe disporre di dati esatti per ottenere risultati precisi. Pertanto, il titolare dovrebbe garantire che i dati utilizzati per addestrare l'IA siano esatti.

Presupponendo che la compagnia assicurativa abbia una base giuridica valida per addestrare l'IA utilizzando i dati personali tratti da un sottoinsieme consistente di clienti esistenti, il titolare sceglie una base di clienti che è rappresentativa della popolazione anche per evitare distorsioni sistematiche.

I dati dei clienti, tra cui quelli sul tipo di assicurazione (per esempio un'assicurazione sanitaria, per la casa, per un viaggio, ecc.), oltre ai dati provenienti da registri pubblici cui il titolare ha legittimamente accesso, vengono quindi raccolti dal rispettivo sistema di gestione dei dati. Tutti i dati sono pseudonimizzati prima di essere trasferiti al sistema dedicato all'addestramento del modello di IA.

Per garantire che i dati utilizzati per l'addestramento dell'IA siano il più esatti possibile, il titolare li raccoglie soltanto dalle fonti che contengono

informazioni corrette e aggiornate.

La compagnia assicurativa verifica che l'IA sia attendibile e fornisca risultati non discriminatori durante il suo sviluppo e, infine, prima della distribuzione del prodotto. Quando l'IA è pienamente addestrata e operativa, la compagnia assicurativa utilizza i risultati a supporto delle valutazioni del rischio assicurativo, senza tuttavia affidarsi esclusivamente all'IA per decidere se concedere l'assicurazione, a meno che la decisione non venga adottata in conformità delle eccezioni di cui all'articolo 22, paragrafo 2, del RGPD.

La compagnia assicurativa verificherà inoltre periodicamente i risultati dell'IA per mantenerla affidabile e, ove necessario, adeguare l'algoritmo

Esempio 2

Il titolare è una struttura sanitaria che ricerca metodi per garantire l'integrità e l'esattezza dei dati personali nei suoi registri clienti.

Qualora due diverse persone arrivino presso la struttura sanitaria alla medesima ora e ricevano lo stesso trattamento, si corre il rischio di confonderle se l'unico parametro che le distingue è il nome. Per garantire l'esattezza, il titolare ha bisogno di un identificativo unico per ciascuna persona e quindi di maggiori informazioni rispetto al solo nome del cliente.

La struttura utilizza diversi sistemi che contengono informazioni personali dei clienti e deve assicurare che tali informazioni sul cliente siano corrette, esatte e coerenti in tutti i sistemi in qualunque momento. La struttura ha individuato vari rischi che possono insorgere se le informazioni sono modificate in un sistema ma non negli altri.

Il titolare decide di mitigare il rischio utilizzando una tecnica di hashing che può servire per garantire l'integrità dei dati nel registro dei trattamenti sanitari. A tal fine crea marcature temporali immutabili e crittografiche per le voci del registro dei trattamenti sanitari a cui il cliente è associato, in modo da consentire il riconoscimento, la correlazione e l'eventuale tracciamento di ogni modifica.

3.7 LIMITAZIONE DELLA CONSERVAZIONE

80. Il titolare deve garantire che i dati personali siano conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore a quello necessario per le finalità per le quali i dati personali sono trattati[40].

    È fondamentale che il titolare sappia esattamente quali dati personali sono trattati e perché. La finalità del trattamento è il criterio principale per stabilire la durata della conservazione dei dati personali.

81. Le misure e le garanzie che attuano il principio della limitazione della conservazione integrano i diritti e le libertà degli interessati, in particolare il di-

ritto alla cancellazione e il diritto di opposizione.

82. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi alla limitazione della conservazione, possono figurare:

- cancellazione e anonimizzazione – il titolare dovrebbe disporre di procedure interne e di funzionalità ben definite per la cancellazione e/o l'anonimizzazione dei dati;
- efficacia dell'anonimizzazione/cancellazione – il titolare si assicura che non sia possibile re-identificare i dati anonimizzati o recuperare quelli cancellati e dovrebbe verificare che tali misure funzionino;
- automatizzazione – la cancellazione di determinati dati personali dovrebbe essere automatizzata;
- criteri di conservazione – il titolare deve stabilire la durata della conservazione e quali dati sono necessari per la specifica finalità;
- giustificazione – il titolare deve essere in grado di motivare perché il periodo di conservazione sia necessario per la finalità e per i dati personali in questione, nonché di spiegare le ragioni e i fondamenti giuridici alla base del periodo di conservazione;
- applicazione delle politiche di conservazione – il titolare dovrebbe far valere determinate politiche di conservazione interne e verificare se l'organizzazione le mette in pratica;
- backup/registri di eventi – i titolari devono stabilire quali dati personali e quale periodo di conservazione siano necessari per i backup e i registri di eventi;
- flusso di dati – i titolari dovrebbero prestare attenzione al flusso di dati personali e alla conservazione delle loro copie, cercando di limitarne la conservazione «temporanea».

Esempio

Il titolare raccoglie dati personali e la finalità del trattamento è gestire le iscrizioni degli interessati. I dati personali vengono cancellati quando termina l'iscrizione e non sussiste una base giuridica che imponga l'ulteriore conservazione dei dati.

A tal fine, il titolare definisce innanzitutto una procedura interna per la conservazione e la cancellazione dei dati, in base alla quale i dipendenti cancellano manualmente i dati personali dopo la fine del periodo di conservazione. Il dipendente si attiene alla procedura di cancellare regolarmente e correggere i dati salvati in qualunque dispositivo, backup, registri, e-mail e altri dispositivi di memorizzazione pertinenti.

Per rendere la cancellazione più efficace e meno soggetta a errori, il titolare implementa un meccanismo automatico al fine di cancellare i dati automaticamente, in modo affidabile e più regolare. Il meccanismo è configurato per seguire una determinata procedura per la cancellazione dei dati che avviene poi a intervalli regolari e predefiniti, eliminando i dati personali

da tutti i dispositivi di memorizzazione dell'impresa. Il titolare esamina e verifica periodicamente la procedura di conservazione, garantendo che sia conforme alla politica di conservazione aggiornata.

3.8 INTEGRITÀ E RISERVATEZZA

83. Il principio di integrità e riservatezza prevede la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. La sicurezza dei dati personali richiede misure appropriate concepite per prevenire e gestire incidenti di violazione dei dati, garantire la corretta esecuzione dei compiti di trattamento dei dati e la conformità agli altri principi, nonché facilitare l'esercizio effettivo dei diritti delle persone.
84. Il considerando 78 stabilisce che una delle misure della DPbDD potrebbe consistere nel consentire al titolare di «di creare e migliorare caratteristiche di sicurezza». Parallelamente alle altre misure della DPbDD, il considerando 78 suggerisce una responsabilità dei titolari, ossia quella di valutare costantemente se stiano utilizzando, in qualunque momento, i mezzi appropriati di trattamento e se le misure scelte contrastino effettivamente le vulnerabilità esistenti. Inoltre, i titolari dovrebbero effettuare revisioni periodiche delle misure di sicurezza poste a presidio e tutela dei dati personali, nonché della procedura per la gestione delle violazioni dei dati.
85. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi all'integrità e alla riservatezza, possono figurare:

- sistema di gestione della sicurezza delle informazioni – occorre disporre di uno strumento operativo per gestire le politiche e le procedure per la sicurezza delle informazioni;
- analisi del rischio – valutare i rischi per la sicurezza dei dati personali, considerando l'impatto sui diritti delle persone, e contrastare quelli identificati, nonché, ai fini dell'utilizzo nella valutazione dei rischi, sviluppare e gestire una «modellizzazione delle minacce» esaustiva, sistematica e realistica e un'analisi della superficie di attacco riferita al software specifico così da ridurre i vettori di attacco e le opportunità di sfruttare eventuali punti deboli e vulnerabilità;
- sicurezza fin dalla progettazione – tenere conto non appena possibile dei requisiti di sicurezza nella progettazione e nello sviluppo del sistema, integrando e svolgendo costantemente test pertinenti;
- manutenzione – rivedere e verificare periodicamente il software, l'hardware, i sistemi e i servizi, ecc. per scoprire eventuali vulnerabilità dei sistemi di supporto del trattamento;
- gestione del controllo degli accessi – solo il personale autorizzato che ne ha necessità dovrebbe avere accesso ai dati personali necessari ai loro compiti di trattamento. Inoltre, il titolare dovrebbe differenziare i privilegi di accesso del personale autorizzato;

  - limitazione dell'accesso (agenti) – definire il trattamento dei dati in modo tale che un numero minimo di persone abbia bisogno di accedere ai dati personali per svolgere le proprie funzioni, e limitare l'accesso di conseguenza;
  - limitazione dell'accesso (contenuto) – nel contesto di ciascuna operazione di trattamento, limitare l'accesso per ogni set di dati ai soli attributi che sono necessari allo svolgimento di tale operazione. Limitare inoltre l'accesso ai dati relativi agli interessati di competenza del rispettivo dipendente;
  - segregazione dell'accesso – definire il trattamento dei dati in modo tale che nessuno necessiti di accedere a tutti i dati raccolti sull'interessato, tanto meno a tutti i dati personali di una categoria specifica di interessati;
- trasferimenti sicuri – i trasferimenti sono protetti da modifiche e accessi non autorizzati e accidentali;
- conservazione sicura – la conservazione dei dati è protetta da modifiche e accessi non autorizzati. Dovrebbero essere previste procedure per valutare il rischio di conservazione centralizzata o decentrata, e le categorie di dati personali cui si applicano. Alcuni dati potrebbero richiedere misure di sicurezza supplementari rispetto ad altri o l'isolamento da questi ultimi;
- pseudonimizzazione – i dati personali e i backup/registri di eventi dovrebbero essere pseudonimizzati come misura di sicurezza per ridurre al minimo i rischi di potenziali violazioni dei dati, ad esempio utilizzando l'hashing o la cifratura;
- backup/registri di eventi – conservare backup e registri di eventi nella misura necessaria per la sicurezza delle informazioni, utilizzare registri delle attività (audit trails) e il monitoraggio degli eventi come controlli di sicurezza su base routinaria, proteggendoli da modifiche e accessi non autorizzati e accidentali e rivedendoli periodicamente, oltre a gestire in modo tempestivo eventuali incidenti;
- ripristino in caso di disastro (disaster recovery)/continuità operativa – soddisfare i requisiti per il ripristino del sistema informativo in caso di disastro e per la continuità operativa, al fine di ripristinare la disponibilità dei dati personali a seguito di incidenti rilevanti;
- protezione in base al rischio – tutte le categorie di dati personali dovrebbero essere protette con misure adeguate contro il rischio di violazioni della sicurezza. I dati che comportano rischi particolari dovrebbero, ove possibile, essere tenuti separati dagli altri dati personali;
- gestione della risposta in caso di incidenti legati alla sicurezza – occorre disporre di metodologie, procedure e risorse per rilevare, limitare, gestire e segnalare le violazioni dei dati e trarne insegnamenti;
- gestione degli incidenti – al fine di rendere più solido il sistema di trattamento, il titolare deve disporre di procedure per gestire violazioni e incidenti, ivi comprese procedure di notifica quali la gestione delle notifiche (per l'autorità di controllo) e delle informazioni (per gli interessati).

Esempio

Un titolare vuole estrarre grandi quantità di dati personali da un database sanitario contenente cartelle cliniche elettroniche (dei pazienti) e trasferirli su un server dedicato aziendale per trattarli ai fini della garanzia della qualità. L'impresa ha valutato che il rischio legato all'instradamento dei dati estratti verso un server accessibile a tutti i dipendenti è probabilmente elevato per i diritti e le libertà degli interessati. Poiché nell'impresa c'è solo un reparto che deve trattare gli estratti dei dati relativi ai pazienti, il titolare decide di limitare ai dipendenti di quel reparto l'accesso al server dedicato. Inoltre, per ridurre ulteriormente i rischi, i dati saranno pseudonimizzati prima del trasferimento.

Per disciplinare l'accesso e attenuare i possibili danni derivanti da malware, l'impresa decide di segregare la rete e stabilire controlli di accesso al server. Inoltre, istituisce un monitoraggio della sicurezza e sistemi di rilevamento e prevenzione delle intrusioni, inibendoli all'utilizzo abituale. È istituito un sistema di controllo automatizzato per monitorare gli accessi e le modifiche che genera segnalazioni e avvisi automatici quando si configurano determinati eventi riguardanti l'uso. Il titolare garantirà che gli utenti abbiano accesso esclusivamente sulla base del principio 'need to know' (cioè di effettive esigenze informative) e purché siano provvisti di adeguati privilegi di accesso. Ogni utilizzo improprio può essere rilevato facilmente e rapidamente.

Alcuni dei dati estratti devono essere confrontati con quelli nuovi e devono pertanto essere conservati per tre mesi. Il titolare decide di inserirli in banche dati separate sullo stesso server e di utilizzare una cifratura trasparente e con chiave a livello di colonna per conservarli. Le chiavi per la decifratura dei dati nelle colonne sono conservate in appositi moduli di sicurezza che possono essere utilizzati, ma non estratti, solo da personale autorizzato.

La presenza di meccanismi per la gestione degli incidenti futuri rende il sistema più solido e affidabile. Il titolare del trattamento è consapevole della necessità di integrare garanzie e misure efficaci e preventive in tutti i trattamenti di dati personali, sia correnti sia futuri, e che così facendo si possono prevenire future violazioni dei dati.

Il titolare stabilisce queste misure di sicurezza per garantire l'esattezza, l'integrità e la riservatezza, ma anche per prevenire la diffusione di malware attraverso attacchi informatici e ottenere una soluzione robusta. Disporre di solide misure di sicurezza contribuisce a instaurare un clima di fiducia con gli interessati.

3.9 RESPONSABILIZZAZIONE[41]

86. Il principio di responsabilizzazione prevede che il titolare sia responsabile

della conformità a tutti i principi summenzionati e sia in grado di dimostrarla.

87. Il titolare deve essere in grado di dimostrare la conformità ai principi; in tal modo può comprovare gli effetti delle misure adottate per tutelare i diritti degli interessati e i motivi per cui tali misure sono considerate adeguate ed efficaci, dimostrando ad esempio in che modo una determinata misura sia adeguata a garantire efficacemente il principio di limitazione della conservazione.

88. Per poter trattare i dati responsabilmente, il titolare dovrebbe sia conoscere le norme in materia di protezione dei dati sia essere in grado di darvi attuazione . Ciò comporta che egli comprenda gli obblighi in materia di protezione dei dati imposti nei suoi riguardi dal RGPD e sia in grado di adempiere a tali obblighi.

4. ARTICOLO 25, PARAGRAFO 3: CERTIFICAZIONE

89. Ai sensi dell'articolo 25, paragrafo 3, la certificazione di cui all'articolo 42 può essere utilizzata come un elemento per dimostrare la conformità con la DPbDD. Parimenti, i documenti che attestano la conformità con la DPbDD potrebbero risultare utili durante una procedura di certificazione. Ciò significa che laddove un trattamento svolto da un titolare o un responsabile sia stato certificato ai sensi dell'articolo 42, le autorità di controllo ne tengono conto nella loro valutazione della conformità con il RGPD, in particolare con la DPbDD.

90. Quando un trattamento è certificato a norma dell'articolo 42, gli elementi che contribuiscono ad attestare la conformità all'articolo 25, paragrafi 1 e 2 sono le procedure di progettazione, ossia la procedura per determinare i mezzi di trattamento, la governance nonché le misure tecniche e organizzative finalizzate ad attuare i principi di protezione dei dati. I criteri di una certificazione in materia di protezione dei dati sono definiti dagli organismi di certificazione o dai titolari dello schema di certificazione e poi approvati dall'autorità di controllo competente o dall'EDPB. Per ulteriori informazioni sui meccanismi di certificazione, rinviamo il lettore alle Linee guida dell'EDPB relative alla certificazione[42] e ad altri orientamenti pertinenti pubblicati sul sito web dell'EDPB.

91. Anche qualora un trattamento sia certificato ai sensi dell'articolo 42, il titolare è comunque tenuto a garantire il monitoraggio costante e il miglioramento della conformità ai criteri della DPbDD di cui all'articolo 25.

5. MISURE PRESE IN ATTUAZIONE DELL'ARTICOLO 25 E RELATIVE CONSEGUENZE

92. Le autorità di controllo possono valutare la conformità con l'articolo 25 secondo le procedure indicate all'articolo 58. I poteri correttivi sono evidenziati all'articolo 58, paragrafo 2, e comprendono avvertimenti, ammonimenti,

ingiunzioni di conformarsi ai diritti degli interessati, limitazioni o divieti di trattamento, sanzioni amministrative pecuniarie, ecc.

93. La DPbDD costituisce, inoltre, un elemento preso in considerazione al fine di stabilire l'entità delle sanzioni pecuniarie per le violazioni del RGPD, cfr. articolo 83, paragrafo 4[43] [44].

6. RACCOMANDAZIONI

94. Benché non siano direttamente destinatari delle disposizioni di cui all'articolo 25, anche i responsabili del trattamento e i produttori rappresentano figure essenziali ai fini della DPbDD e dovrebbero essere consapevoli del fatto che i titolari sono tenuti a trattare i dati personali solo utilizzando sistemi e tecnologie che integrano i principi di protezione dei dati.

95. Nel trattare i dati per conto dei titolari, o nel fornire ai titolari soluzioni di trattamento, responsabili e produttori dovrebbero utilizzare le loro competenze per instaurare un clima di fiducia e orientare i loro clienti, PMI comprese, verso soluzioni di progettazione che integrano la protezione dei dati nel trattamento. Ciò significa a sua volta che la progettazione di prodotti e servizi dovrebbe semplificare le esigenze dei titolari.

96. Nell'applicare l'articolo 25 si dovrebbe tener presente che il principale obiettivo di progettazione è costituito dall' integrare nelle misure adeguate per lo specifico trattamento l'efficace attuazione dei principi e la tutela dei diritti degli interessati. Al fine di agevolare e potenziare l'adozione della DPbDD, formuliamo le seguenti raccomandazioni per i titolari, i produttori e i responsabili del trattamento:

- i titolari dovrebbero pensare alla protezione dei dati sin dalle *fasi iniziali* della pianificazione di un trattamento e ancor prima di definirne i mezzi;
- se un titolare è coadiuvato da un responsabile della protezione dei dati (RPD), l'EDPB incoraggia il coinvolgimento attivo dell'RDP per integrare la DPbDD nelle procedure di acquisizione e sviluppo, nonché lungo l'intero ciclo di vita del trattamento;
- un trattamento può essere *certificato*. La capacità di ottenere una certificazione per il trattamento rappresenta un valore aggiunto per il titolare al momento di scegliere tra i diversi software, hardware, servizi e/o sistemi di trattamento forniti dai produttori o dai responsabili del trattamento. Pertanto, i produttori dovrebbero sforzarsi di dimostrare che la DPbDD è parte integrante del ciclo di vita dello sviluppo della loro soluzione per il trattamento; una certificazione può inoltre orientare gli interessati nella loro scelta tra i diversi prodotti e servizi: avere la possibilità di far certificare un trattamento può costituire da vantaggio competitivo per i produttori, i responsabili e i titolari e può persino accrescere la fiducia degli interessati nel trattamento dei loro dati personali. In assenza di certificazione, i titolari dovrebbero cercare di avere altre *garanzie* in merito alla conformità ai requisiti della DPbDD da parte dei produttori o dei responsabili del trattamento;

- titolari, responsabili e produttori dovrebbero tenere conto degli obblighi di fornire una tutela specifica ai minori e ad altri gruppi vulnerabili, nel rispetto della DPbDD;
- produttori e responsabili dovrebbero cercare di agevolare l'attuazione della DPbDD al fine di supportare il titolare nell'adempimento degli obblighi previsti dall'articolo 25. I titolari, d'altro canto, non dovrebbero scegliere produttori o responsabili che non offrono sistemi in grado di consentire o facilitare l'adempimento degli obblighi di cui all'articolo 25 in capo ai titolari stessi, poiché saranno questi ultimi a rispondere dell'eventuale mancata attuazione;
- i produttori e i responsabili dovrebbero svolgere un ruolo attivo nel garantire che siano soddisfatti i criteri relativi allo «stato dell'arte» e notificare ai titolari del trattamento qualunque modifica a tale «stato dell'arte» che possa compromettere l'efficacia delle misure adottate. I titolari dovrebbero inserire questo requisito fra le clausole contrattuali per assicurarsi un tempestivo aggiornamento;
- l'EDPB raccomanda ai titolari di richiedere che i produttori e i responsabili del trattamento dimostrino in che modo i loro hardware, software, servizi o sistemi permettano al titolare di soddisfare i requisiti in materia di responsabilizzazione in conformità della DPbDD, per esempio utilizzando indicatori chiave di prestazione (KPI) per dimostrare l'efficacia delle misure e delle garanzie nell'attuazione dei principi e dei diritti;
- l'EDPB sottolinea la necessità di un approccio armonizzato per attuare i principi e i diritti in modo efficace e invita anche le associazioni o gli organismi che elaborano codici di condotta a norma dell'articolo 40 a incorporarvi orientamenti in materia di DPbDD specifici per il singolo settore;
- i titolari dovrebbero essere corretti e trasparenti nei confronti degli interessati per quanto concerne la valutazione e dimostrazione dell'effettiva attuazione della DPbDD, analogamente a quanto si verifica nella dimostrazione della loro conformità con il RGPD in base al principio di responsabilizzazione;
- le tecnologie di rafforzamento della privacy (PET, privacy-enhancing technologies) che hanno raggiunto lo stato dell'arte possono essere utilizzate fra le misure da adottare in conformità dei requisiti della DPbDD, se del caso, secondo un approccio basato sul rischio. Di per sé, le PET non coprono necessariamente gli obblighi di cui all'articolo 25. I titolari devono valutare se la specifica misura sia adeguata ed efficace ai fini dell'attuazione dei principi di protezione dei dati e dei diritti degli interessati;
- i sistemi preesistenti sono soggetti agli stessi obblighi in materia di DPbDD ai quali soggiacciono i sistemi nuovi, cosicché, ove non siano già conformi ai principi della DPbDD e non sia possibile effettuare modifiche per adempiere ai relativi obblighi, i sistemi preesistenti non sono conformi agli obblighi del RGPD e non possono essere utilizzati per trattare dati personali;
- l'articolo 25 non prevede requisiti meno stringenti per le PMI. Le indicazioni fornite di seguito possono facilitare le PMI nel garantire la conformità all'articolo 25 :

  1. eseguire una valutazione dei rischi in fase precoce;

2. cominciare dal trattamento di piccole quantità di dati, passando poi gradatamente a trattamenti di maggiore portata e complessità;
3. cercare di ottenere garanzie in materia di DPbDD da parte dei produttori e dei responsabili del trattamento, quali ad esempio la certificazione e l'adesione a codici di condotta;
4. avvalersi di partner di provata affidabilità;
5. rivolgersi alle autorità di protezione dei dati;
6. leggere gli orientamenti delle suddette autorità e dell'EDPB;
7. attenersi ai codici di condotta, ove disponibili;
8. richiedere assistenza e consulenza professionali.

Per il comitato europeo per la protezione dei dati
La presidente

(Andrea Jelinek)

NOTE

[1] Le interpretazioni qui contenute si applicano anche all'articolo 20 della direttiva (UE) 2016/680 e all'articolo 27 del regolamento 2018/1725.

[2] Il considerando 78 del RGPD indica chiaramente questa necessità: «*In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati.*»

[3] La questione relativa all'«efficacia» è affrontata di seguito al sottocapitolo 2.1.2.

[4] Definita all'articolo 4, paragrafo 5, del RGPD.

[5] Cfr. il considerando 4 del RGPD.

[6] «I principi fondamentali applicabili ai titolari del trattamento (ossia legittimità, minimizzazione dei dati, limitazione delle finalità, trasparenza, integrità dei dati, esattezza dei dati) dovrebbero rimanere gli stessi indipendentemente dal trattamento e dai rischi per gli interessati. Tuttavia, la dovuta considerazione della natura e dell'ambito di tale trattamento è sempre stata parte integrante dell'applicazione di questi principi affinché siano intrinsecamente scalabili». Gruppo di lavoro "Articolo 29", «Statement on the role of a risk-based approach in data protection legal frameworks», WP 218, 30 maggio 2014, pag. 3, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[7] Cfr. i considerando 74 e 78.

[8] Cfr. decisione «Kalkar» della Corte costituzionale federale tedesca nel 1978: https://germanlawarchive.iuscomp.org/?p=67 che può offrire un fondamento metodologico per una definizione oggettiva del concetto. Su tale fondamento, lo "stato dell'arte" in termini di livello tecnologico si collocherebbe tra il livello tecnologico delle «conoscenze e ricerche scientifiche esistenti» e le più consolidate «regole tecniche generalmente riconosciute». Lo «stato dell'arte» può quindi essere identificato nel livello tecnologico di un servizio, una tecnologia o un prodotto come esistenti sul mercato e in grado di conseguire gli obiettivi individuati nel modo più efficace.

[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

[11] Ne sono esempi le categorie particolari di dati personali, il processo decisionale automatizzato, i rapporti di forza asimmetrici, l'imprevedibilità del trattamento, la difficoltà per l'interessato di esercitare i propri diritti, ecc.

[12] Gruppo di lavoro dell'articolo 29, «Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679», WP 248 rev. 01, 4 ottobre 2017, ec.europa.eu/newsroom/document.cfm?doc_id=47711 - approvate dall'EDPB.

[13] Articolo 5, paragrafo 1, lettere da b) a e) del RGPD.

[14] EDPS, «Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection», 25 febbraio 2019, edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

[15] Cfr. anche EDPS, «Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit» , https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

[16] Per maggiori informazioni in merito alla necessità, cfr. il documento del Gruppo di lavoro "Articolo 29", «Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE», WP 217, 9 aprile 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf

[17] Ai sensi dell'articolo 4, paragrafo 2, del RGPD, il trattamento include la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il

raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

[18] Gruppo di lavoro dell'articolo 29, «Parere 05/2014 sulle tecniche di anonimizzazione», WP 216, 10 aprile 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf

[19] Cfr. articolo 4, paragrafo 1, del RGDP, considerando 26 del RGDP, Gruppo di lavoro "Articolo 29", «Parere 05/2014 sulle tecniche di anonimizzazione». Si veda anche la sottosezione sulla «limitazione della conservazione» alla sezione 3 del presente documento, che indica la necessità da parte del titolare di garantire l'efficacia delle tecniche di anonimizzazione attuate.

[20] Cfr. causa Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia n. 931/13.,

[21] Si possono trovare maggiori esempi nel documento dell'autorità norvegese per la protezione dei dati. «Software Development with Data Protection by Design and by Default» (Sviluppo di software con protezione dei dati fin dalla progettazione e protezione per impostazione predefinita). 28 novembre 2017. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729

[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers

[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

[24] Approfondimenti su come interpretare il concetto di trasparenza si possono trovare nel documento del Gruppo di lavoro dell'articolo 29, «Linee guida sulla trasparenza ai sensi del regolamento 2016/679», WP 260 rev. 01, 11 aprile 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 - approvate dall'EDPB.

[25] L'autorità francese per la protezione dei dati ha pubblicato diversi esempi che illustrano le migliori prassi su come informare gli utenti nonché altri principi di trasparenza: https://design.cnil.fr/en/

[26] EDPB, «Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati», versione 2.0, 8 ottobre 2019, edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_it.pdf

[27] Cfr. sezione sulla limitazione delle finalità di seguito.

[28] Cfr. le Linee guida 05/2020 sul consenso a norma del regolamento 2016/679, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_it

[29] Cfr. le Linee guida 05/2020 sul consenso a norma del regolamento 2016/679, pag. 24, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_it

[30] Se il consenso è la base giuridica originaria, cfr. le Linee guida 05/2020 sul consenso a norma del regolamento 2016/679, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_it

[31] Cfr. articolo 6, paragrafo 1, lettera b), del RGPD.

[32] Cfr. le Linee guida in materia di processi decisionali automatizzati relativi alle persone fisiche e profilazione ai fini del regolamento 2016/679, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826

[33] Cfr. il considerando 71 del RGPD.

[34] Il Gruppo di lavoro "Articolo 29" ha elaborato linee guida per comprendere il principio della limitazione delle finalità ai sensi della direttiva 95/46/CE. Sebbene il parere non sia adottato dall'EDPB, può tuttavia essere pertinente in quanto il principio è formulato in termini identici a quelli di cui al RGPD. Gruppo di lavoro"Articolo 29", «Opinion 03/2013 on purpose limitation», WP 203, 2 aprile 2013, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_it.pdf

[35] Articolo 5, paragrafo 1, lettera b) del RGPD.

[36] Articolo 5, paragrafo 1, lettera c) del RGPD.

[37] Il considerando 39 del RGPD stabilisce quanto segue: «[...] I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi.»

[38] Articolo 5, paragrafo 1, lettera d), del RGPD.

[39] Cfr. il considerando 65.

[40] Articolo 5, paragrafo 1, lettera c) del RGPD.

[41] Cfr. il considerando 74, in base a cui i titolari sono tenuti a dimostrare l'efficacia delle loro misure.

[42] EDPB, «Linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento», versione 3.0, 4 giugno 2019,

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_it.pdf

[43] Ai sensi dell'articolo 83, paragrafo 2, lettera d), del RGPD, nel determinare l'imposizione delle sanzioni per violazione dello stesso RGPD «si tiene debito conto» del «grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32».

[44] Sono disponibili maggiori informazioni sulle sanzioni nel documento del Gruppo di lavoro dell'articolo 29, «Guidelines on application and setting of administrative fines for the purposes of the Regulation 2016/679», WP 253, 3 ottobre 2017, ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 - approvate dall'EDPB.

Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità Versione 2.0

Adottate il 9 marzo 2021

Cronologia delle versioni

Versione 2.0	9 marzo 2021	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	28 gennaio 2020	Adozione delle linee guida per consultazione pubblica

Indice

1 Introduzione
- 1.1 Lavori correlati
- 1.2 Diritto applicabile
- 1.3 Ambito di applicazione
- 1.4 Definizioni
- 1.5 Rischi relativi alla tutela della vita privata e alla protezione dei dati

2 Raccomandazioni generali
- 2.1 Categorie di dati
- 2.2 Finalità
- 2.3 Pertinenza e minimizzazione dei dati
- 2.4 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita
- 2.5 Informazione
- 2.6 Diritti dell'interessato
- 2.7 Sicurezza
- 2.8 Trasferimento di dati personali a terzi
- 2.9 Trasferimento di dati personali al di fuori dell'UE/del SEE
- 2.10 Uso di tecnologie Wi-Fi di bordo

3 Studi di casi
- 3.1 Prestazione di un servizio da parte di un terzo
- 3.2 eCall
- 3.3 Studi sull'incidentalità
- 3.4 Furto d'auto

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI,

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito "GDPR"),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

visti gli articoli 12 e 22 del proprio regolamento interno,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

1. INTRODUZIONE

1. Simbolo dell'economia del XX secolo, l'automobile è uno dei beni di consumo di massa che hanno influenzato la società nel suo complesso. Solitamente associate al concetto di libertà, le automobili sono spesso considerate più di un semplice mezzo di trasporto. Di fatto esse rappresentano un ambito privato in cui le persone possono godere di una certa autonomia decisionale al riparo da interferenze esterne. Oggi, mentre i veicoli connessi si apprestano a diventare prodotti di largo consumo, tale visione non corrisponde più alla realtà. La connettività di bordo si sta rapidamente estendendo dai modelli di lusso e dai marchi di fascia alta ai modelli di fascia media realizzati in grandi quantità e i veicoli si stanno trasformando in enormi hub di dati. Non solo i veicoli ma anche i conducenti e i passeggeri sono sempre più connessi. Infatti molti modelli lanciati sul mercato negli ultimi anni integrano sensori e apparecchiature di bordo connesse, capaci di raccogliere e registrare, tra l'altro, le prestazioni del motore, le abitudini di guida, i luoghi visitati e, potenzialmente, persino i movimenti oculari del conducente, la frequenza cardiaca oppure dati biometrici al fine di identificare in maniera univoca una data persona fisica[2].

2. Il trattamento di questi dati avviene in un ecosistema complesso, che non è limitato agli operatori tradizionali del settore automobilistico ma è anche plasmato dall'emergere di nuovi operatori dell'economia digitale. Questi nuovi operatori potranno offrire servizi di *infotainment* quali musica online, informazioni sul traffico e sulle condizioni stradali, oppure fornire sistemi e servizi di assistenza alla guida, ad esempio software di guida autonoma, aggiornamenti sullo stato del veicolo, assicurazioni basate sull'uso (*usage-based*) o mappatura dinamica. Inoltre poiché i veicoli sono connessi tramite reti di comunicazione elettronica, anche i gestori delle infrastrutture stradali e gli operatori di telecomunicazione coinvolti in questo processo svolgono un ruolo importante per quanto riguarda le potenziali operazioni di trattamento che interessano i dati personali di conducenti e passeggeri.

3. Inoltre i veicoli connessi stanno generando crescenti quantità di dati che possono essere considerati, per la maggior parte, dati personali in quanto riferiti a conducenti o passeggeri. Anche qualora non siano direttamente correlati a un nominativo ma si riferiscano ad aspetti tecnici e a caratteristiche del veicolo, i dati raccolti da un'automobile connessa riguarderanno comunque il conducente o i passeggeri. A titolo di esempio i dati riguardanti lo stile di guida o la distanza percorsa, i dati relativi all'usura di parti del veicolo, i dati relativi all'ubicazione o quelli raccolti da videocamere possono riguardare il comportamento del conducente nonché informazioni concernenti altre persone che potrebbero trovarsi all'interno del veicolo, oppure interessati che si trovano nelle vicinanze. Tali dati tecnici sono prodotti da una persona fisica e consentono la sua identificazione diretta o indiretta da parte del titolare del trattamento o di un terzo. Il veicolo può essere considerato un terminale utilizzabile da diversi utenti. Pertanto, come accade per i personal computer, questa potenziale pluralità di utenti non influisce sulla natura personale dei dati.

4. Nel 2016 la Fédération Internationale de l'Automobile (FIA) ha organizzato una campagna a livello europeo dal titolo "My Car My Data" per sondare l'opinione dei cittadini europei riguardo alle automobili connesse[3]. La campagna ha rivelato un forte interesse dei conducenti nei confronti della connettività ma ha anche evidenziato la necessità di esercitare una sorveglianza sull'uso dei dati prodotti dai veicoli e l'importanza di ottemperare alla normativa in materia di protezione dei dati personali. Per ciascuna delle parti interessate la sfida consiste dunque nell'integrare la dimensione della "protezione dei dati personali" sin dalla fase di progettazione del prodotto e nell'offrire trasparenza agli utilizzatori di automobili oltre alla possibilità di esercitare il controllo in relazione ai loro dati come previsto al considerando 78 del GDPR. Tale approccio contribuisce a rafforzare la fiducia degli utenti e dunque lo sviluppo a lungo termine di tali tecnologie.

1.1 LAVORI CORRELATI

5. I veicoli connessi sono ampiamente diventati oggetto di regolamentazione nell'ultimo decennio, in particolare negli ultimi due anni. A livello nazionale e internazionale sono stati dunque pubblicati vari lavori in materia di sicurezza e privacy dei veicoli connessi. Tali normative e iniziative mirano a integrare con norme settoriali i quadri esistenti in materia di protezione dei dati e di tutela della vita privata o a fornire orientamenti ai professionisti.

1.1.1 INIZIATIVE A LIVELLO EUROPEO E INTERNAZIONALE

6. A decorrere dal 31 marzo 2018 un sistema eCall di bordo basato sul 112 è obbligatorio su tutti i nuovi tipi di veicoli M1 e N1 (autovetture e veicoli leggeri)[4,5]. Nel 2006 il Gruppo di lavoro Articolo 29 aveva già adottato un documento di lavoro sulle implicazioni in materia di protezione dei dati e rispetto della vita privata dell'iniziativa eCall[6]. Inoltre, come discusso in precedenza, ad ottobre del 2017 il Gruppo di lavoro Articolo 29 ha adottato un parere sul trattamento dei dati personali nel contesto dei sistemi di trasporto intelligente cooperativi (C-ITS).
7. A gennaio del 2017 l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) ha pubblicato uno studio incentrato sulla cibersicurezza e sulla resilienza delle automobili intelligenti che elenca i componenti sensibili nonché le minacce, i rischi e i fattori di attenuazione corrispondenti e le possibili misure di sicurezza da attuare[7]. A settembre del 2017 la conferenza internazionale dei commissari in materia di protezione dei dati e della vita privata (ICDPPC) ha adottato una risoluzione sui veicoli connessi[8]. Infine, ad aprile del 2018 anche il gruppo di lavoro internazionale sulla tutela dei dati nelle telecomunicazioni (IWGDPT) ha adottato un documento di lavoro sui veicoli connessi[9].

1.1.2 INIZIATIVE NAZIONALI DEI MEMBRI DEL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI (EDPB)

8. A gennaio del 2016 la conferenza delle autorità tedesche federali e statali per la protezione dei dati e l'associazione tedesca dell'industria automobilistica (VDA) hanno pubblicato una dichiarazione comune sui principi della protezione dei dati nei veicoli connessi e non connessi[10]. Ad agosto del 2017 il Centre for Connected and Autonomous Vehicles (CCAV) britannico ha pubblicato un documento di orientamento che stabilisce i principi della cibersicurezza per i veicoli connessi e automatizzati al fine di sensibilizzare alla questione il settore automobilistico[11]. Ad ottobre del 2017 l'autorità francese per la protezione dei dati, la Commission Nationale de l'Informatique et des Libertés (CNIL), ha pubblicato un pacchetto di conformità per le automobili connesse allo scopo di fornire alle parti interessate una serie di indicazioni su come integrare la protezione dei dati fin dalla progettazione e per impostazione predefinita in modo che gli interessati possano esercitare un controllo efficace sui dati che li riguardano[12].

1.2 DIRITTO APPLICABILE

9. Il quadro giuridico dell'UE pertinente è costituito dal GDPR, che si applica ogniqualvolta un trattamento di dati nel contesto dei veicoli connessi comporti il trattamento di dati personali di persone fisiche.
10. Oltre al GDPR, la direttiva 2002/58/CE, riveduta dalla direttiva 2009/136/CE (di seguito "direttiva e-privacy"), **definisce una norma specifica per tutti gli operatori che intendono archiviare informazioni o accedere a informazioni archiviate nell'apparecchiatura terminale di un abbonato o di un utente nello Spazio economico europeo (SEE)**.
11. Di fatto sebbene la maggioranza delle disposizioni contenute nella direttiva e-privacy (articolo 6, articolo 9 ecc.) si applichi soltanto ai fornitori di servizi di comunicazione elettronica accessibili al pubblico e ai fornitori di reti pubbliche di comunicazione, l'articolo 5, paragrafo 3, della direttiva e-privacy costituisce una disposizione di carattere generale. Esso si applica non soltanto ai servizi di comunicazione elettronica ma anche a qualsiasi soggetto, sia esso pubblico o privato, che registri o legga informazioni su un'apparecchiatura terminale indipendentemente dalla natura dei dati che sono archiviati o a cui si accede.
12. Per quanto riguarda il concetto di "apparecchiatura terminale", la definizione è fornita dalla direttiva 2008/63/CE[13]. L'articolo 1, lettera a), definisce le apparecchiature terminali come "*le apparecchiature allacciate direttamente o indirettamente all'interfaccia di una rete pubblica di telecomunicazioni per trasmettere, trattare o ricevere informazioni; in entrambi i casi di allacciamento, diretto o indiretto, esso può essere realizzato via cavo, fibra ottica o via elettromagnetica; un allacciamento è indiretto se l'apparecchiatura è interposta fra il terminale e l'inter-*

faccia della rete pubblica; b) le apparecchiature delle stazioni terrestri per i collegamenti via satellite".

13. Pertanto, a condizione che siano soddisfatti i suddetti criteri, il veicolo connesso e il dispositivo ad esso collegato dovrebbero essere considerati "*apparecchiature terminali*" (alla stregua di un computer, di uno smartphone o di una smart TV) e trovano applicazione, ove pertinente, le disposizioni dell'articolo 5, paragrafo 3, della direttiva e-privacy.

14. Come delineato dall'EDPB nel parere 5/2019 sull'interazione tra la direttiva e-privacy e il GDPR[14], l'articolo 5, paragrafo 3, della direttiva e-privacy prevede che, di norma, e fatte salve le deroghe a detta norma di cui al punto 17 in appresso, l'archiviazione di informazioni o l'accesso ad informazioni già archiviate nell'apparecchiatura terminale di un abbonato o utente richiedano il suo consenso preliminare. Nella misura in cui le informazioni archiviate nel dispositivo dell'utente finale costituiscono dati personali, l'articolo 5, paragrafo 3, della direttiva e-privacy prevale sull'articolo 6 del GDPR con riguardo alle attività di archiviazione di o accesso a tali informazioni[15]. Qualunque operazione di trattamento di dati personali successiva alle operazioni di trattamento di cui sopra, compreso il trattamento di dati personali ottenuti mediante l'accesso a informazioni nell'apparecchiatura terminale, per essere lecita deve avere un fondamento giuridico a norma dell'articolo 6 del GDPR[16].

15. Poiché, al momento di richiedere il consenso all'archiviazione delle informazioni o all'accesso alle stesse a norma dell'articolo 5, paragrafo 3, della direttiva e-privacy, il titolare del trattamento dovrà comunicare all'interessato tutte le finalità del trattamento, compreso qualsiasi trattamento successivo alle operazioni di cui sopra (ossia il "trattamento successivo"), il consenso a norma dell'articolo 6 del GDPR costituirà in genere il fondamento giuridico più adeguato su cui basare il trattamento dei dati personali successivo a dette operazioni (nella misura in cui la finalità del trattamento successivo sia compresa dall'interessato che esprime il suo consenso, cfr. i punti 53-54 in appresso). Pertanto il consenso costituirà probabilmente il fondamento giuridico sia per l'archiviazione delle informazioni e l'accesso alle informazioni già archiviate sia per il trattamento successivo di dati personali[17]. Di fatto nel valutare l'osservanza dell'articolo 6 del GDPR si dovrebbe tenere conto del fatto che il trattamento nel suo complesso comporta specifiche attività per le quali il legislatore dell'UE ha cercato di offrire un'ulteriore tutela[18]. Inoltre, nell'individuare la base giuridica appropriata, i titolari del trattamento devono tenere conto dell'impatto sui diritti degli interessati in maniera da rispettare il principio di correttezza[19]. La conclusione è che i titolari del trattamento non possono invocare l'articolo 6 del GDPR per ridurre l'ulteriore tutela offerta dall'articolo 5, paragrafo 3, della direttiva e-privacy.

16. L'EDPB ricorda che il concetto di consenso nella direttiva e-privacy corrisponde al concetto di consenso nel GDPR e deve soddisfare tutti i requisiti e le condizioni per il consenso di cui all'articolo 4, punto 11, e all'articolo 7 del GDPR.

17. Sebbene il principio fondante sia costituito dal consenso, l'articolo 5, paragrafo 3, della direttiva e-privacy consente tuttavia di esonerare l'archiviazione di informazioni o l'accesso a informazioni già archiviate nell'apparecchiatura terminale dall'obbligo del consenso informato qualora l'operazione soddisfi uno dei criteri seguenti:

- **deroga 1**: abbia luogo al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica;
- **deroga 2**: abbia luogo nella misura strettamente necessaria per consentire al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente di erogare tale servizio.

18. In tali casi il trattamento di dati personali, compresi i dati personali ottenuti mediante l'accesso a informazioni archiviate nell'apparecchiatura terminale, si fonda su una delle basi giuridiche fornite dall'articolo 6 del GDPR. Ad esempio il consenso non è richiesto laddove il trattamento dei dati sia necessario per fornire servizi di navigazione GPS richiesti dall'interessato qualora tali servizi siano qualificabili come servizi della società dell'informazione.

1.3 AMBITO DI APPLICAZIONE

19. L'EDPB desidera sottolineare che le presenti linee guida intendono facilitare l'osservanza della normativa in rapporto al trattamento di dati personali effettuato da un'ampia gamma di parti interessate che operano in questo contesto. Il presente documento, tuttavia, non è finalizzato a illustrare tutti i casi d'uso possibili in tale contesto, né a fornire orientamenti per ogni possibile situazione specifica.

20. Il presente documento si concentra, in particolare, sul trattamento dei dati personali in relazione all'uso non professionale di veicoli connessi da parte degli interessati: conducenti, passeggeri, proprietari di veicoli, altri utenti della strada ecc. Più specificamente il documento riguarda i dati personali: i) trattati all'interno del veicolo, ii) scambiati tra il veicolo e i dispositivi personali ad esso connessi (ad esempio lo smartphone dell'utente) oppure iii) raccolti localmente nel veicolo ed esportati verso soggetti esterni (ad esempio case costruttrici, gestori di infrastrutture, imprese di assicurazione, officine di riparazione) ai fini di un ulteriore trattamento.

21. Nel presente documento la definizione di veicolo connesso deve essere interpretata in senso lato. Il veicolo connesso può essere definito come un veicolo dotato di numerose centraline elettroniche di controllo (ECU) collegate tra loro per mezzo di una rete di bordo, nonché di strumenti di connettività che consentono di condividere informazioni con altri dispositivi interni ed esterni al veicolo. Ciò consente lo scambio di dati tra il veicolo e i dispositivi personali ad esso collegati, ad esempio per il *mirroring* delle applicazioni mobili sull'unità di informazione e intrattenimento in-dash [sul cruscotto] della vettura. Inoltre lo sviluppo di applicazioni mobili *stand-alone*, ossia indipendenti dal veicolo (ad esempio basate esclusivamente sull'utilizzo dello smartphone), che forniscono assistenza ai conducenti, rientra nell'oggetto

del presente documento, in quanto tali applicazioni contribuiscono a determinare le capacità di connettività del veicolo anche qualora, di fatto, non si basino di per sé sullo scambio di dati con il veicolo stesso. Le applicazioni per i veicoli connessi sono molteplici e diversificate. Di seguito se ne forniscono alcuni esempi[20].

22. *Gestione della mobilità*: funzioni che consentono ai conducenti di raggiungere la destinazione in tempi brevi e in maniera efficiente sul piano dei costi, fornendo informazioni tempestive riguardanti la navigazione GPS, la presenza di condizioni ambientali potenzialmente pericolose (ad esempio ghiaccio sulle strade), la congestione del traffico o la presenza di lavori stradali, parcheggi o autofficine, il consumo ottimizzato del carburante o i pedaggi stradali.
23. *Gestione del veicolo*: funzioni intese ad aiutare i conducenti a ridurre i costi d'esercizio e a migliorare la facilità di utilizzo, ad esempio avvisi sullo stato del veicolo e avvisi di manutenzione programmata, trasferimento dei dati relativi all'utilizzo (ad esempio per i servizi di riparazione del veicolo), assicurazioni personalizzate di tipo "*Pay As/How You Drive*", operazioni a distanza (ad esempio impianto di riscaldamento) o configurazioni del profilo (ad esempio posizionamento dei sedili).
24. *Sicurezza stradale*: funzioni che avvisano il conducente riguardo a pericoli esterni e risposte interne, ad esempio protezione in caso di collisione, avvisi di pericolo, avvisi di deviazione dalla corsia di marcia, rilevamento della stanchezza del conducente, chiamata d'emergenza (eCall) o "scatole nere" (registratori di dati relativi ad eventi incidentali) utilizzate a fini di indagine.
25. *Intrattenimento*: funzioni che forniscono informazioni e offrono intrattenimento al conducente e ai passeggeri, ad esempio interfacce con gli smartphone (chiamate telefoniche a mani libere, SMS vocali), hotspot WLAN, musica, video, internet, social media, servizi di *mobile office* o servizi di "domotica".
26. *Assistenza alla guida*: funzioni che comportano l'automazione parziale o totale della guida, ad esempio assistenza operativa o guida autonoma in presenza di traffico intenso, nelle manovre di parcheggio o sulle autostrade.
27. *Benessere*: funzioni che monitorano il comfort del conducente, la sua capacità di guidare e la sua idoneità alla guida, come ad esempio il rilevamento della stanchezza o l'assistenza medica.
28. Pertanto i veicoli possono nascere già connessi o no e i dati personali possono essere raccolti con mezzi diversi, ossia: i) sensori di bordo, ii) *telematic box* o iii) applicazioni mobili (ad esempio accessibili da un dispositivo appartenente al conducente). Per rientrare nell'ambito di applicazione del presente documento le applicazioni mobili devono essere correlate all'ambiente di guida. Ad esempio le applicazioni di navigazione GPS rientrano nell'ambito del presente documento. Sono invece escluse dall'ambito delle presenti linee guida le applicazioni le cui funzionalità si limitano a suggerire ai conducenti luoghi di interesse (ristoranti, monumenti storici ecc.).
29. Molti dei dati generati da un veicolo connesso riguardano persone fisiche

identificate o identificabili e pertanto costituiscono dati personali. Ad esempio i dati comprendono dati direttamente identificativi (come l'identità completa del conducente) e dati indirettamente identificativi, quali informazioni dettagliate sui viaggi effettuati, i dati sull'utilizzo del veicolo (riguardanti, ad esempio, lo stile di guida o la distanza percorsa) o i dati tecnici del veicolo (ad esempio dati relativi all'usura di parti del veicolo), che, messi in relazione con altri dati e soprattutto con il numero di identificazione del veicolo (VIN), possono permettere di risalire a una persona fisica. I dati personali nei veicoli connessi possono comprendere anche metadati, ad esempio relativi allo stato di manutenzione del veicolo. In altri termini qualunque dato associabile a una persona fisica rientra quindi nell'ambito di applicazione del presente documento.

30. L'ecosistema del veicolo connesso comprende un'ampia gamma di operatori interessati. Più precisamente tale ecosistema comprende operatori tradizionali del settore automobilistico e operatori emergenti del settore digitale. Le presenti linee guida sono pertanto rivolte alle case costruttrici di veicoli, ai produttori di accessori e ai fornitori di componenti, ai riparatori di autoveicoli, alle concessionarie automobilistiche, ai fornitori di servizi automobilistici, ai gestori di parchi veicoli, alle compagnie di assicurazione dei veicoli a motore, ai fornitori di servizi di intrattenimento, agli operatori di telecomunicazioni, ai gestori di infrastrutture stradali e alle amministrazioni pubbliche, nonché agli interessati. L'EDPB sottolinea che le categorie di interessati saranno diverse in rapporto al singolo servizio (ad esempio conducenti, proprietari, passeggeri ecc.). Il suddetto elenco non è esaustivo, in quanto l'ecosistema è costituito da una vasta gamma di servizi, alcuni dei quali richiedono l'autenticazione o l'identificazione diretta mentre altri non necessitano di autenticazione o identificazione.

31. Alcuni trattamenti di dati da parte di persone fisiche all'interno del veicolo sono effettuati *"per l'esercizio di attività a carattere esclusivamente personale o domestico"* e di conseguenza sono esclusi dall'ambito di applicazione del GDPR[21]. Ciò riguarda, in particolare, l'uso esclusivo di dati personali all'interno del veicolo da parte degli interessati che li hanno trasmessi al quadro strumenti del veicolo. Tuttavia l'EDPB ricorda che, conformemente al considerando 18, il GDPR *"si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico"*.

1.3.1 QUALI OPERAZIONI NON RIENTRANO NELL'AMBITO DI APPLICAZIONE DEL PRESENTE DOCUMENTO

32. I datori di lavoro che forniscono autovetture aziendali ai loro dipendenti potrebbero decidere di monitorare le azioni dei dipendenti (ad esempio per garantire la sicurezza del dipendente, delle merci o dei veicoli, per assegnare risorse, per tenere traccia di un servizio e addebitarne il costo o per controllare le ore di lavoro). Il trattamento di dati effettuato dai datori di lavoro in tale contesto solleva considerazioni che attengono specificamente all'ambito

dei rapporti di lavoro e che potrebbero essere disciplinate da normative del lavoro a livello nazionale sulle quali le presenti linee guida non possono soffermarsi[22].

33. Anche se il trattamento di dati nel contesto dei veicoli commerciali destinati all'uso professionale (ad esempio trasporto pubblico), dei trasporti condivisi e della soluzione MaaS (Mobility-as-a-Service) potrebbe sollevare considerazioni specifiche che esulano dall'ambito di applicazione delle presenti linee guida generali, molti dei principi e delle raccomandazioni formulati nel presente documento saranno applicabili anche a tali tipologie di trattamento.

34. Poiché sono sistemi abilitati alla connessione radio, i veicoli connessi sono soggetti al tracciamento passivo, ad esempio al tracciamento Wi-Fi o Bluetooth. In tal senso non differiscono da altri dispositivi connessi e rientrano nell'ambito di applicazione della direttiva e-privacy, che è attualmente in fase di revisione. Ne consegue che è esclusa dall'ambito del presente documento anche la localizzazione su vasta scala di veicoli dotati di connessione Wi-Fi[23] da parte di soggetti che transitano o sostano in prossimità del veicolo e che utilizzano i comuni servizi di localizzazione degli smartphone. Tali servizi comunicano regolarmente ai server centrali tutte le reti Wi-Fi visibili. Poiché il Wi-Fi integrato può essere considerato un identificativo secondario del veicolo[24], vi è il rischio di una raccolta sistematica e continuativa di profili completi degli spostamenti dei veicoli.

35. Sempre più spesso i veicoli sono dotati di dispositivi per la registrazione di immagini (ad esempio telecamere di assistenza al parcheggio o *dashcam*). Poiché ciò si ricollega al problema delle riprese effettuate in luoghi pubblici, che esige una valutazione del quadro legislativo pertinente, specifico di ciascuno Stato membro, tale trattamento di dati non rientra nell'ambito di applicazione delle presenti linee guida.

36. Il trattamento di dati nel contesto dei sistemi di trasporto intelligenti cooperativi (C-ITS), quali definiti nella direttiva 2010/40/UE[25], è stato oggetto di un parere specifico del Gruppo di lavoro Articolo 29[26]. Sebbene la definizione del concetto di C-ITS nella direttiva non contenga specifiche tecniche, nel suo parere il Gruppo di lavoro Articolo 29 si concentra sulle comunicazioni a corto raggio, ossia quelle che non comportano l'intervento di un operatore di rete. Più specificamente esso fornisce un'analisi per casi di utilizzo specifici con riguardo alla fase iniziale di attuazione e si è impegnato a valutare in una fase successiva le nuove questioni che certamente sorgeranno con l'attuazione di livelli di automazione più elevati. Poiché le implicazioni per la protezione dei dati nel contesto del C-ITS sono molto specifiche (quantitativi di dati senza precedenti sull'ubicazione, trasmissione continua di dati personali, scambio di dati tra veicoli e altre infrastrutture di trasporto ecc.) e il tema è tuttora oggetto di discussione a livello europeo, il trattamento di dati personali in tale contesto esula dall'ambito di applicazione delle presenti linee guida.

37. Infine il presente documento non mira ad affrontare tutte le possibili questioni e i possibili interrogativi sollevati dai veicoli connessi e non può essere pertanto considerato esaustivo.

1.4 DEFINIZIONI

38. Il **trattamento** di dati personali comprende qualsiasi operazione che riguardi dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione ecc.[27].

39. L'**interessato** è la persona fisica a cui si riferiscono i dati che sono oggetto di trattamento. Nel contesto dei veicoli connessi potrà trattarsi, in particolare, del conducente (principale o occasionale), del passeggero o del proprietario del veicolo[28].

40. Il **titolare del trattamento** è la persona che determina le finalità e i mezzi del trattamento che ha luogo nei veicoli connessi[29]. I titolari del trattamento possono essere i fornitori di servizi che trattano i dati del veicolo per trasmettere al conducente informazioni sul traffico, messaggi relativi alla guida ecologica o avvisi sul funzionamento del veicolo, oppure imprese di assicurazione che offrono contratti a consumo di tipo "*Pay As You Drive*" o costruttori di veicoli che raccolgono dati sull'usura di parti del veicolo per migliorarne la qualità. A norma dell'articolo 26 del GDPR, due o più titolari possono determinare congiuntamente le finalità e i mezzi del trattamento ed essere pertanto considerati contitolari del trattamento. In tal caso essi devono definire con chiarezza i rispettivi obblighi, con particolare riguardo all'esercizio dei diritti degli interessati e alla comunicazione delle informazioni di cui agli articoli 13 e 14 del GDPR.

41. Il **responsabile del trattamento** è chiunque tratti dati personali in nome e per conto del titolare del trattamento[30]. Il responsabile del trattamento raccoglie e tratta i dati secondo le istruzioni del titolare del trattamento, senza utilizzare tali dati per i propri scopi. A titolo di esempio in alcuni casi è possibile che i costruttori di accessori e i fornitori di componenti trattino dati per conto dei costruttori di veicoli (il che non implica che non possano essere titolari del trattamento per altre finalità). Oltre a stabilire che i responsabili del trattamento devono mettere in atto misure tecniche e organizzative adeguate in modo tale da garantire un livello di sicurezza idoneo al rischio, l'articolo 28 del GDPR definisce gli obblighi dei responsabili del trattamento.

42. Per **destinatario** si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi[31]. A titolo di esempio un partner commerciale del fornitore di servizi che riceva da quest'ultimo dati personali generati dal veicolo è destinatario di dati personali e, indipendentemente dal fatto che funga da nuovo titolare del trattamento o da responsabile del trattamento, è tenuto ad adempiere tutti gli obblighi imposti dal GDPR.

43. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari[32]; il tratta-

mento di tali dati da parte di dette autorità pubbliche deve essere conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento. Ad esempio le autorità di contrasto sono terzi autorizzati quando richiedono dati personali nell'ambito di un'indagine conformemente al diritto dell'Unione o degli Stati membri.

1.5 RISCHI RELATIVI ALLA TUTELA DELLA VITA PRIVATA E ALLA PROTEZIONE DEI DATI

44. Il Gruppo di lavoro Articolo 29 ha già espresso diverse preoccupazioni in merito ai sistemi del cosiddetto internet degli oggetti (*Internet of Things* - IoT) che possono essere estese anche ai veicoli connessi[33]. I problemi relativi alla sicurezza e al controllo dei dati, già sottolineati in relazione all'IoT, sono ancora più cruciali nel contesto dei veicoli connessi, giacché attengono a questioni di sicurezza stradale (e possono avere un impatto sull'integrità fisica del conducente) in un contesto tradizionalmente percepito come isolato e protetto da interferenze esterne.
45. Inoltre i veicoli connessi sollevano serie preoccupazioni per la tutela della vita privata e la protezione dei dati per quanto concerne il trattamento di dati relativi all'ubicazione, in quanto il carattere sempre più invasivo di questo trattamento può mettere a dura prova le attuali possibilità di mantenere l'anonimato. L'EDPB desidera porre un particolare accento e sensibilizzare le parti interessate sul fatto che l'utilizzo di tecnologie di localizzazione esige l'introduzione di specifiche tutele al fine di impedire la sorveglianza delle persone e l'abuso dei dati.

1.5.1 MANCANZA DI CONTROLLO E ASIMMETRIA INFORMATIVA

46. I conducenti e i passeggeri dei veicoli potrebbero non essere sempre adeguatamente informati in merito al trattamento dei dati che ha luogo all'interno o per mezzo di un veicolo connesso. È possibile che le informazioni siano fornite soltanto al proprietario del veicolo, che potrebbe non essere il conducente, e che inoltre non siano fornite in maniera tempestiva. Esiste dunque il rischio che le funzionalità o le opzioni offerte non siano sufficienti per esercitare il controllo necessario affinché le persone interessate possano avvalersi del loro diritto al rispetto della vita privata e alla protezione dei dati. Si tratta di un aspetto importante in quanto, nel corso della loro vita utile, i veicoli potrebbero appartenere a più di un proprietario perché sono venduti o perché, anziché essere acquistati, sono acquisiti in leasing.
47. Inoltre la comunicazione nel veicolo può essere avviata automaticamente e tramite impostazioni predefinite, senza che il diretto interessato ne sia al corrente. In assenza della possibilità di controllare efficacemente l'interazione tra il veicolo e le apparecchiature ad esso connesse, il controllo del flusso di dati da parte dell'utente è destinato a diventare estremamente difficile. Sarà ancora più difficile controllarne l'uso successivo per evitare il rischio di una "eterogenesi di funzioni" (*function creep*).

1.5.2 QUALITÀ DEL CONSENSO DELL'UTENTE

48. L'EDPB sottolinea che, laddove il trattamento dei dati sia basato sul consenso, devono essere rispettati tutti gli elementi che rendono valido tale consenso; ciò significa che il consenso deve essere libero, specifico e informato e costituisce una manifestazione di volontà inequivocabile dell'interessato, secondo l'interpretazione fornita nelle linee guida dell'EDPB sul consenso[34]. I titolari del trattamento devono prestare molta attenzione alle modalità di ottenimento di un consenso valido presso i vari partecipanti, quali i proprietari o gli utilizzatori di autovetture. Tale consenso deve essere prestato separatamente, per finalità specifiche e non può essere accorpato al contratto di acquisto o leasing di una nuova autovettura. Il consenso deve poter essere revocato con la stessa facilità con cui lo si è espresso.
49. Lo stesso principio deve essere applicato quando il consenso è necessario per ottemperare alla direttiva e-privacy, ad esempio in caso di archiviazione di informazioni o di accesso a informazioni già archiviate nel veicolo, come previsto in taluni casi dall'articolo 5, paragrafo 3, di tale direttiva. Infatti, come già sottolineato, in tale contesto il consenso deve essere interpretato alla luce del GDPR.
50. In molti casi l'utente potrebbe non essere consapevole del trattamento dei dati effettuato nel suo veicolo. Tale mancanza di informazione costituisce un ostacolo rilevante quando si tratta di dimostrare la validità del consenso ai sensi del GDPR, giacché il consenso deve essere informato. In tali circostanze il consenso non può essere utilizzato come base giuridica per il corrispondente trattamento dei dati a norma del GDPR.
51. I meccanismi tipicamente utilizzati per ottenere il consenso delle persone possono risultare di difficile applicazione nel contesto dei veicoli connessi. Ne risulta un consenso "di bassa qualità", basato su un'informazione carente, oppure l'impossibilità concreta di prestare un consenso ben calibrato che tenga conto delle preferenze individuali. Nella pratica può essere difficile ottenere il consenso anche laddove conducenti e passeggeri non abbiano alcun rapporto col proprietario del veicolo, come nel caso di veicoli di seconda mano, acquisiti in leasing, noleggiati o presi in prestito.
52. Nei casi in cui la direttiva e-privacy non richiede il consenso dell'interessato, il titolare del trattamento ha comunque la responsabilità di scegliere, ai sensi dell'articolo 6 del GDPR, il fondamento giuridico più adatto al caso per il trattamento dei dati personali.

1.5.3 ULTERIORE TRATTAMENTO DI DATI PERSONALI

53. Quando sono raccolti sulla base del consenso a norma dell'articolo 5, paragrafo 3, della direttiva e-privacy o sulla base di una delle deroghe di cui all'articolo 5, paragrafo 3 e sono successivamente trattati conformemente all'articolo 6 del GDPR, i dati possono essere sottoposti a un ulteriore trattamento soltanto se il titolare del trattamento chiede un ulteriore consenso per tale

finalità diversa o è in grado di dimostrare che il trattamento è basato sul diritto dell'Unione o degli Stati membri ai fini della salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, del GDPR[35]. L'EDPB ritiene che l'ulteriore trattamento sulla base della verifica di compatibilità ai sensi dell'articolo 6, paragrafo 4, del GDPR non sia possibile in tali casi, in quanto pregiudicherebbe il livello di protezione dei dati offerto dalla direttiva e-privacy. Infatti il consenso, ove previsto dalla direttiva e-privacy, deve essere specifico e informato; ciò significa che gli interessati devono essere al corrente della finalità di ciascun trattamento di dati e avere il diritto di rifiutare finalità specifiche[36]. Il fatto di ritenere possibile l'ulteriore trattamento sulla base di una verifica di compatibilità ai sensi dell'articolo 6, paragrafo 4, del GDPR eluderebbe il principio stesso dei requisiti del consenso stabiliti dalla direttiva vigente.

54. L'EDPB ricorda che il consenso iniziale non legittimerà mai l'ulteriore trattamento, in quanto il consenso è valido solo se informato e specifico.

55. Ad esempio i dati di telemetria, che sono raccolti durante l'utilizzo del veicolo a scopo di manutenzione, non possono essere comunicati alle compagnie di assicurazione dei veicoli a motore senza il consenso degli utenti ai fini della profilazione dei conducenti e della conseguente offerta di polizze assicurative basate sulla condotta di guida.

56. Inoltre i dati raccolti dai veicoli connessi possono essere trattati dalle autorità di contrasto per rilevare violazioni dei limiti di velocità o altre infrazioni se e quando sono soddisfatte le condizioni specifiche della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie. In questo caso tali dati saranno considerati relativi a condanne penali e reati in base alle condizioni stabilite dall'articolo 10 del GDPR e dalla legislazione nazionale eventualmente applicabile. I costruttori possono fornire tali dati alle autorità di contrasto qualora siano soddisfatte le condizioni specifiche per tale trattamento. L'EDPB sottolinea che il trattamento di dati personali effettuato al solo scopo di soddisfare le richieste delle autorità di contrasto non costituisce una finalità determinata, esplicita e legittima ai sensi dell'articolo 5, paragrafo 1, lettera b), del GDPR. Quando sono autorizzate dalla legge, le autorità di contrasto potrebbero costituire "terzi" ai sensi dell'articolo 4, punto 10, del GDPR; in questo caso i costruttori sarebbero autorizzati a trasmettere loro i dati di cui dispongono nel rispetto delle disposizioni di legge pertinenti di ciascuno Stato membro.

1.5.4 RACCOLTA DI DATI ECCEDENTI

57. Il continuo aumento del numero di sensori integrati nei veicoli connessi comporta il rischio assai elevato di una raccolta di dati eccedenti rispetto a quelli necessari allo scopo.

58. Lo sviluppo di nuove funzionalità, più specificamente quelle basate su algoritmi di apprendimento automatico (*machine learning*), potrebbe rendere necessaria la raccolta di una grande quantità di dati per un periodo di tempo prolungato.

1.5.5 SICUREZZA DEI DATI PERSONALI

59. L'ampia gamma di funzionalità, servizi e interfacce (ad esempio web, USB, RFID, Wi-Fi) offerta dai veicoli connessi aumenta la superficie di attacco e dunque il numero di vulnerabilità potenziali attraverso cui i dati personali potrebbero essere compromessi. A differenza della maggioranza dei dispositivi IoT, i veicoli connessi sono sistemi critici in cui una violazione della sicurezza potrebbe mettere a repentaglio la vita degli utilizzatori e delle persone che si trovano nelle vicinanze. È dunque ancora più importante affrontare il rischio rappresentato dalla possibilità che gli hacker tentino di sfruttare le vulnerabilità dei veicoli connessi.
60. Inoltre i dati personali memorizzati nei veicoli e/o in ambiti esterni (ad esempio le infrastrutture di *cloud computing*) devono essere adeguatamente protetti dall'accesso non autorizzato. Ad esempio durante un intervento di manutenzione il veicolo sarà affidato a un meccanico che avrà bisogno di accedere ad alcuni dati tecnici. Il meccanico deve poter accedere ai dati tecnici, ma potrebbe tentare di accedere a tutti i dati memorizzati nel veicolo.

2. RACCOMANDAZIONI GENERALI

61. Al fine di attenuare i suddetti rischi per gli interessati, si invitano produttori di veicoli e di accessori, fornitori di servizi e ogni altra parte interessata che agisca in qualità di titolare o di responsabile del trattamento in relazione ai veicoli connessi a seguire alcune raccomandazioni di carattere generale formulate nei paragrafi seguenti.

2.1 CATEGORIE DI DATI

62. Come osservato nell'introduzione, i dati associati ai veicoli connessi saranno da ritenersi per la maggior parte dati personali nella misura in cui sono riconducibili ad una o più persone identificabili. Ciò vale anche per i dati tecnici relativi agli spostamenti del veicolo (ad esempio velocità o distanza percorsa) e allo stato del veicolo (ad esempio temperatura del liquido di raffreddamento del motore, regime del motore, pressione degli pneumatici). Taluni dati generati dai veicoli connessi potrebbero meritare particolare attenzione anche per via della loro sensibilità e/o del loro potenziale impatto sui diritti e sugli interessi degli interessati. L'EDPB ha individuato tre categorie di dati personali su cui i produttori di veicoli e accessori, i fornitori di servizi e altri titolari del trattamento dovrebbero porre particolare attenzione: dati relativi all'ubicazione, dati biometrici (e qualsiasi categoria particolare di dati di cui all'articolo 9 del GDPR) e dati che potrebbero rivelare reati o violazioni del codice della strada.

2.1.1 DATI RELATIVI ALL'UBICAZIONE

63. Nella raccolta di dati personali i produttori di veicoli e accessori, i fornitori di servizi e altri titolari del trattamento dovrebbero tenere presente che i dati relativi all'ubicazione sono particolarmente atti a fornire indicazioni sulle abitudini di vita degli interessati. I viaggi effettuati hanno la particolare caratteristica di permettere di risalire al luogo di lavoro e di residenza, nonché ai centri di interesse (svago) del conducente e possono eventualmente rivelare informazioni sensibili quali il credo religioso (attraverso il luogo di culto) oppure l'orientamento sessuale (sulla base dei luoghi visitati). Pertanto i produttori di veicoli e accessori, i fornitori di servizi e altri titolari del trattamento dovrebbero avere cura di non raccogliere dati relativi all'ubicazione tranne qualora ciò sia assolutamente necessario per la finalità del trattamento. A titolo di esempio, laddove il trattamento consista nell'individuare il movimento del veicolo, il giroscopio è sufficiente allo scopo e non è necessario raccogliere dati relativi all'ubicazione.

64. In generale la raccolta di dati relativi all'ubicazione deve rispettare anche i principi seguenti:

- configurazione adeguata della frequenza di accesso ai dati relativi all'ubicazione, e del loro livello di dettaglio, in relazione alla finalità del trattamento. Ad esempio un'applicazione per le previsioni del tempo non dovrebbe essere in grado di accedere ogni secondo alla posizione del veicolo, nemmeno qualora l'interessato abbia espresso il proprio consenso;
- comunicazione di informazioni accurate sulla finalità del trattamento (ad esempio la cronologia delle localizzazioni è conservata? Se lo è, a che scopo?);
- quando il trattamento è basato sul consenso, ottenimento di un consenso valido (libero, specifico e informato) che sia distinto dalle condizioni generali di vendita o di utilizzo, ad esempio sul computer di bordo;
- attivazione della localizzazione non per impostazione predefinita e in maniera continuativa fin dall'avvio del veicolo, ma soltanto quando l'utente attiva una funzionalità che richiede di localizzare il veicolo;
- comunicazione all'utente del fatto che la funzione di localizzazione è stata attivata, in particolare mediante l'utilizzo di icone (ad esempio una freccia che si sposta sul display);
- possibilità di disattivare la localizzazione in qualsiasi momento;
- definizione di un periodo di conservazione limitato.

2.1.2 DATI BIOMETRICI

65. Nel contesto dei veicoli connessi i dati biometrici utilizzati al fine di identificare in modo univoco una persona fisica possono essere trattati, tra l'altro, limitatamente a quanto previsto dall'articolo 9 del GDPR e in base alle deroghe nazionali, per consentire l'accesso a un veicolo, l'autenticazione del conducente/proprietario e/o l'accesso alle impostazioni del profilo e alle preferenze

del conducente. Nel valutare il possibile utilizzo di dati biometrici, al fine di garantire all'interessato il pieno controllo sui dati che lo riguardano è necessario, da un lato, prevedere l'esistenza di un'alternativa non biometrica (ad esempio l'utilizzo di una chiave o di un codice) senza ulteriori vincoli (in altri termini l'uso di dati biometrici non dovrebbe essere obbligatorio) e, dall'altro lato, conservare e confrontare il modello biometrico in forma cifrata solo a livello locale, senza che i dati biometrici siano trattati da un terminale di lettura/raffronto esterno.

66. Nel caso dei dati biometrici[37] è importante garantire che la soluzione di autenticazione biometrica sia sufficientemente affidabile, in particolare rispettando i principi seguenti:

- l'adeguamento della soluzione biometrica utilizzata (ad esempio il tasso di falsi positivi e falsi negativi) è funzionale al livello di sicurezza del controllo degli accessi richiesto;
- la soluzione biometrica utilizzata si basa su un sensore resistente agli attacchi (ad esempio utilizzo di impronte piane per il riconoscimento delle impronte digitali);
- il numero di tentativi di autenticazione è limitato;
- il modello biometrico è memorizzato nel veicolo in forma cifrata utilizzando un algoritmo crittografico e una gestione delle chiavi adeguati allo stato dell'arte;
- i dati grezzi utilizzati per l'elaborazione del modello biometrico e per l'autenticazione dell'utente sono trattati in tempo reale senza mai essere archiviati, neppure localmente.

2.1.3 DATI CHE RIVELANO REATI O ALTRE VIOLAZIONI

67. Ai fini del trattamento di dati relativi a potenziali reati ai sensi dell'articolo 10 del GDPR, l'EDPB raccomanda di ricorrere al trattamento locale dei dati, sul quale l'interessato ha il pieno controllo (cfr. le considerazioni relative al trattamento locale nella sezione 2.4). In realtà, fatte salve alcune eccezioni (cfr. gli studi sull'incidentalità illustrati nella sezione 3.3), il trattamento esterno di dati che rivelano reati o altre violazioni è vietato. Pertanto in base alla sensibilità dei dati è necessario porre in essere misure di sicurezza efficaci come quelle descritte nella sezione 2.7, al fine di offrire una protezione contro l'accesso, la modifica e la cancellazione illeciti di tali dati.

68. Alcune categorie di dati personali provenienti dai veicoli connessi potrebbero rivelare che è stato commesso o è in corso di commissione un reato o un altro tipo di violazione ("dati relativi ai reati") e pertanto potrebbero essere soggette a particolari restrizioni (ad esempio dati indicanti che il veicolo ha oltrepassato una striscia bianca, dati relativi alla velocità istantanea di un veicolo combinati con dati sulla localizzazione esatta). In particolare qualora tali dati siano trattati dalle autorità nazionali competenti a fini di indagine penale e perseguimento di reati, si applicherebbero le garanzie previste all'articolo 10 del GDPR.

2.2 FINALITÀ

69. I dati personali possono essere trattati per una vasta gamma di finalità in relazione ai veicoli connessi, tra cui la sicurezza del conducente, l'assicurazione, il trasporto efficiente, l'intrattenimento o i servizi di informazione. Conformemente al GDPR i titolari del trattamento devono garantire che le finalità perseguite siano "determinate, esplicite e legittime", che i dati siano successivamente trattati in un modo che non sia incompatibile con tali finalità e che vi sia una valida base giuridica per il trattamento secondo quanto previsto all'articolo 5 del GDPR. Alcuni esempi concreti di finalità perseguite dai titolari del trattamento che operano nel contesto dei veicoli connessi sono illustrati nella parte III delle presenti linee guida, in cui sono inoltre formulate raccomandazioni specifiche per ciascuna tipologia di trattamento.

2.3 PERTINENZA E MINIMIZZAZIONE DEI DATI

70. Al fine di rispettare il principio della minimizzazione dei dati[38] i produttori di veicoli e accessori, i fornitori di servizi e altri titolari del trattamento dovrebbero prestare particolare attenzione alle categorie di dati che essi hanno la necessità di ottenere da un veicolo connesso, giacché sono tenuti a raccogliere soltanto dati personali pertinenti e necessari al trattamento. Ad esempio i dati relativi all'ubicazione sono particolarmente invasivi e possono rivelare molte delle abitudini di vita degli interessati. Pertanto gli operatori del settore dovrebbero avere particolare cura di evitare la raccolta di dati relativi all'ubicazione tranne qualora essa sia assolutamente necessaria rispetto alla finalità del trattamento (cfr. la sezione 2.1. e le considerazioni ivi contenute riguardo ai dati relativi all'ubicazione).

2.4 PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

71. Tenuto conto del volume e della varietà dei dati personali generati dai veicoli connessi, l'EDPB rileva che i titolari del trattamento sono tenuti a garantire che le tecnologie utilizzate nel contesto dei veicoli connessi siano configurate in maniera da rispettare la vita privata delle persone applicando gli obblighi in materia di protezione dei dati fin dalla progettazione e per impostazione predefinita di cui all'articolo 25 del GDPR. Le tecnologie dovrebbero essere progettate in modo da minimizzare la raccolta di dati personali, fornire impostazioni predefinite a tutela della vita privata e garantire che gli interessati siano correttamente informati e abbiano la possibilità di modificare agevolmente le configurazioni associate ai loro dati personali. A beneficio del settore e dei fornitori terzi di applicazioni potrebbe essere utile fornire orientamenti specifici sulle modalità con cui case produttrici e fornitori di servizi possono adempiere agli obblighi in materia di protezione dei dati fin dalla progettazione e per impostazione predefinita.

72. Talune prassi di carattere generale, descritte in appresso, possono anch'esse contribuire a ridurre i rischi per i diritti e le libertà delle persone fisiche associati ai veicoli connessi[39].

2.4.1 TRATTAMENTO LOCALE DI DATI PERSONALI

73. In generale i produttori di veicoli e accessori, i fornitori di servizi e altri titolari del trattamento dovrebbero, per quanto possibile, utilizzare processi che non prevedano l'uso di dati personali o il trasferimento di dati personali all'esterno del veicolo (ossia i dati dovrebbero essere trattati internamente). Tuttavia, per loro stessa natura, i veicoli connessi presentano di fatto alcuni rischi, ad esempio la possibilità di attacchi al trattamento svolto in sede locale da parte di soggetti esterni, o fughe di dati locali mediante la vendita di parti del veicolo. È dunque opportuno prestare particolare attenzione e prevedere l'adozione di misure di sicurezza adeguate per garantire che i dati continuino ad essere trattati solo localmente. Tale scenario offre il vantaggio di garantire all'utente il pieno ed esclusivo controllo dei dati personali che lo riguardano e, per tale ragione, presenta, "fin dalla progettazione", minori rischi per la tutela della vita privata soprattutto perché vieta alle parti interessate di effettuare il trattamento all'insaputa dell'interessato. Esso consente inoltre il trattamento di dati sensibili, quali dati biometrici o dati relativi a reati o altre violazioni, nonché di dati dettagliati relativi all'ubicazione, che sarebbe altrimenti soggetto a norme più stringenti (cfr. in appresso). Analogamente tale approccio presenta minori rischi per la cibersicurezza e comporta una minore latenza, il che lo rende particolarmente indicato per le funzioni di assistenza alla guida automatizzata. Di seguito si forniscono alcuni esempi di questo tipo di soluzione:

- applicazioni di guida ecologica che trattano dati nel veicolo per mostrare in tempo reale sul display di bordo consigli in materia di guida ecologica;
- applicazioni che comportano il trasferimento di dati personali a un dispositivo come ad esempio uno smartphone sotto il pieno controllo dell'utente (ad esempio tramite Bluetooth o Wi-Fi) e nelle quali i dati del veicolo non sono trasmessi al fornitore dell'applicazione o al produttore del veicolo; un esempio potrebbe essere costituito dall'associazione dello smartphone per l'utilizzo del display della vettura, dei sistemi multimediali, del microfono (o di altri sensori) per le telefonate ecc., nella misura in cui i dati raccolti rimangano sotto il controllo dell'interessato e siano utilizzati esclusivamente per fornire il servizio da questi richiesto;
- applicazioni di bordo per il miglioramento della sicurezza, ad esempio quelle che prevedono la trasmissione di segnali acustici o di vibrazioni del volante quando il conducente sorpassa una vettura senza azionare la freccia o supera una linea bianca, o che forniscono avvisi sullo stato del veicolo (ad esempio sull'usura delle pastiglie dei freni);
- applicazioni per lo sblocco, l'avvio e/o l'attivazione di determinati comandi del veicolo mediante i dati biometrici del conducente memorizzati all'interno del veicolo (ad esempio modelli facciali o vocali o particolarità delle impronte digitali).

74. Applicazioni come quelle sopra indicate comportano un trattamento effettuato da una persona fisica per l'esercizio di attività a carattere esclusivamente personale (ossia senza il trasferimento di dati personali a un titolare o a un responsabile del trattamento). In conformità con l'articolo 2, paragrafo 2, del GDPR, **tali applicazioni esulano pertanto dall'ambito di applicazione del GDPR**.

75. Tuttavia, sebbene il GDPR non si applichi ai trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico, conformemente al suo considerando 18 esso si applica invece ai titolari o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico (produttori automobilistici, fornitori di servizi ecc.). Quando agiscono in qualità di titolari o di responsabili del trattamento, tali soggetti devono pertanto sviluppare un'applicazione di bordo sicura, nel rispetto del principio di tutela della vita privata fin dalla progettazione e per impostazione predefinita. Ad ogni modo, conformemente al considerando 78 del GDPR *"(i)n fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati"*[40]. Da un lato questo processo migliorerà lo sviluppo di servizi incentrati sull'utente e, dall'altro lato, faciliterà e consentirà in futuro eventuali utilizzi successivi che potrebbero rientrare nell'ambito di applicazione del GDPR. Più specificamente l'EDPB raccomanda di sviluppare una piattaforma applicativa di bordo sicura, fisicamente separata dalle funzioni della vettura legate alla sicurezza, affinché l'accesso ai dati del veicolo non dipenda da capacità cloud esterne non necessarie.

76. Ogniqualvolta possibile, i produttori di autovetture e i fornitori di servizi dovrebbero prendere in considerazione la possibilità di un trattamento locale dei dati al fine di attenuare i rischi potenziali del trattamento in cloud, quali delineati nel parere sul cloud computing del Gruppo di lavoro Articolo 29[41].

77. In generale gli utenti dovrebbero essere in grado di controllare la modalità con cui i propri dati sono raccolti e trattati all'interno del veicolo:

- le informazioni relative al trattamento devono essere fornite nella lingua del conducente (manuale, impostazioni ecc.);
- l'EDPB raccomanda di sottoporre a trattamento, per impostazione predefinita, soltanto i dati strettamente necessari al funzionamento del veicolo. Gli interessati dovrebbero avere la possibilità di attivare o disattivare il trattamento dei dati per ogni altra finalità e da parte di ogni altro titolare/responsabile del trattamento nonché di cancellare i dati in questione, tenendo conto della finalità e della base giuridica del trattamento;
- i dati non dovrebbero essere trasmessi a terzi (ossia l'utente ha accesso esclusivo ai dati);

- i dati dovrebbero essere conservati soltanto per il periodo di tempo necessario alla prestazione del servizio o secondo quanto altrimenti previsto dal diritto dell'Unione o degli Stati membri;
- gli interessati dovrebbero essere in grado di cancellare definitivamente qualsiasi dato personale prima che i veicoli siano messi in vendita;
- gli interessati dovrebbero, ove fattibile, avere un accesso diretto ai dati generati da tali applicazioni.

78. Infine, sebbene non sia sempre possibile ricorrere al trattamento locale per ogni caso d'uso, spesso potrà essere predisposto un "trattamento ibrido". Ad esempio, nel contesto dell'assicurazione basata sull'uso del veicolo, i dati personali relativi alla condotta di guida (ad esempio la forza esercitata sul pedale del freno, il chilometraggio percorso ecc.) potrebbero essere trattati all'interno del veicolo oppure dal fornitore di servizi telematici per conto dell'impresa di assicurazione (il titolare del trattamento) così da generare punteggi numerici da trasmettere a quest'ultima con una frequenza prestabilita (ad esempio su base mensile). In tal modo l'impresa di assicurazione non avrà accesso ai dati grezzi sulla condotta di guida ma potrà accedere soltanto al punteggio aggregato, che è il risultato del trattamento. Il rispetto del principio di minimizzazione dei dati è così garantito sin dalla progettazione. Ciò significa anche che gli utenti devono avere la possibilità di esercitare i loro diritti quando i dati sono conservati da altri soggetti: ad esempio l'utente dovrebbe avere la possibilità di cancellare i dati conservati nei sistemi di un'officina di riparazione o di una concessionaria alle condizioni stabilite dall'articolo 17 del GDPR.

2.4.2 ANONIMIZZAZIONE E PSEUDONIMIZZAZIONE

79. Qualora sia prevista la trasmissione di dati personali all'esterno del veicolo, sarebbe opportuno valutare la possibilità di renderli anonimi prima della loro trasmissione. In fase di anonimizzazione il titolare del trattamento dovrebbe tenere conto di tutti i trattamenti che potrebbero potenzialmente condurre alla re-identificazione dei dati, ad esempio la trasmissione di dati anonimizzati localmente. L'EDPB ricorda che i principi di protezione dei dati non si applicano alle informazioni anonime, vale a dire alle informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato[42]. Una volta che un insieme di dati è reso effettivamente anonimo e le persone non sono più identificabili, le norme europee in materia di protezione dei dati non sono più applicabili. Pertanto l'anonimizzazione, ove pertinente, potrebbe costituire una strategia valida per preservare i vantaggi e attenuare i rischi relativi ai veicoli connessi.
80. Come precisato nel parere del Gruppo di lavoro Articolo 29 sulle tecniche di anonimizzazione, per conseguire l'anonimizzazione dei dati si possono utilizzare vari metodi, talvolta in combinazione tra loro[43].
81. Altre tecniche come ad esempio la pseudonimizzazione[44] possono contribu-

ire a ridurre i rischi generati dal trattamento dei dati, tenendo conto che, nella maggioranza dei casi, per conseguire la finalità del trattamento non sono necessari dati direttamente identificabili. La pseudonimizzazione, se rafforzata da garanzie di sicurezza, migliora la protezione dei dati personali riducendo i rischi di abuso. A differenza dell'anonimizzazione, la pseudonimizzazione è reversibile e i dati pseudonimizzati sono considerati dati personali soggetti al GDPR.

2.4.3 VALUTAZIONI D'IMPATTO SULLA PROTEZIONE DEI DATI

82. Alla luce della portata e della sensibilità dei dati personali che possono essere generati attraverso i veicoli connessi è probabile che il trattamento, soprattutto in situazioni nelle quali i dati personali sono trattati all'esterno del veicolo, determini spesso un rischio elevato per i diritti e le libertà delle persone. In tali casi gli operatori del settore saranno tenuti a effettuare una valutazione d'impatto sulla protezione dei dati al fine di individuare e attenuare i rischi secondo quanto previsto agli articoli 35 e 36 del GDPR. Anche laddove la valutazione d'impatto sulla protezione dei dati non sia necessaria, è buona prassi effettuarne una quanto prima nella fase di progettazione. Ciò consentirà agli operatori del settore di integrare i risultati di tale analisi nelle rispettive scelte di progettazione prima della diffusione di nuove tecnologie.

2.5 INFORMAZIONE

83. Prima del trattamento dei dati personali, sono fornite all'interessato informazioni riguardanti l'identità del titolare del trattamento (ad esempio il produttore di veicoli e accessori o il fornitore di servizi), la finalità del trattamento, i destinatari dei dati, il periodo di conservazione dei dati e i diritti dell'interessato a norma del GDPR[45].

84. Inoltre il produttore di veicoli e accessori, il fornitore di servizi e ogni altro titolare del trattamento dovrebbero fornire all'interessato, in termini chiari, semplici e facilmente accessibili, anche le informazioni seguenti:

- i dati di contatto del responsabile della protezione dei dati;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- il riferimento esplicito ai legittimi interessi perseguiti dal titolare del trattamento o da terzi qualora tali legittimi interessi costituiscano la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limi-

tazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

- l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca qualora il trattamento sia basato sul consenso;
- ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e il riferimento alle garanzie utilizzate per il trasferimento;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, che produca effetti giuridici che riguardano l'interessato o che incida in modo analogo significativamente sulla sua persona, e informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. Un tipico esempio potrebbe essere costituito dalla fornitura a persone fisiche di polizze di assicurazione basate sull'uso del veicolo;
- il diritto di proporre reclamo a un'autorità di controllo;
- informazioni relative all'ulteriore trattamento;
- in caso di contitolarità del trattamento, informazioni chiare e complete sulle responsabilità di ciascun titolare del trattamento.

85. In alcuni casi i dati personali non sono raccolti direttamente presso l'interessato. Ad esempio un produttore di veicoli e accessori potrebbe affidare a un concessionario la raccolta di informazioni sul proprietario del veicolo in modo tale da offrire un servizio di assistenza stradale di emergenza. Quando la raccolta dei dati non è diretta, il produttore di veicoli e accessori, il fornitore di servizi o un altro titolare del trattamento, oltre a fornire le informazioni di cui sopra, deve indicare le categorie di dati personali interessati, la provenienza dei dati personali e, se del caso, specificare se tali dati provengono da fonti pubblicamente disponibili. Il titolare del trattamento deve fornire tali informazioni entro un termine ragionevole dall'ottenimento dei dati **e non oltre il più breve fra i termini seguenti** conformemente all'articolo 14, paragrafo 3, del GDPR: i) entro un mese dall'ottenimento dei dati, in considerazione delle specifiche circostanze in cui i dati personali sono trattati, ii) al momento della prima comunicazione all'interessato, oppure iii) se i dati sono trasmessi a un terzo, prima della trasmissione.

86. Potrà inoltre essere necessario fornire nuove informazioni agli interessati nel caso in cui subentri un nuovo titolare del trattamento. Un servizio di assistenza stradale che interagisce con veicoli connessi può essere fornito da diversi titolari del trattamento a seconda del paese o della regione in cui è richiesta l'assistenza. I nuovi titolari del trattamento dovrebbero fornire agli interessati le informazioni necessarie quando questi ultimi si spostano da un paese all'altro e i servizi che interagiscono con i veicoli connessi sono forniti da nuovi titolari del trattamento.

87. Le informazioni possono essere fornite agli interessati secondo un approccio multilivello[46], ossia distinguendo fra due livelli di informazioni: da un lato le informazioni di primo livello, che sono le più importanti per gli interessati e, dall'altro lato, le informazioni che si presume siano di interesse in una fase successiva. Le informazioni essenziali di primo livello comprendono, oltre all'identità del titolare del trattamento, la finalità del trattamento e una descrizione dei diritti dell'interessato, così come ogni altra informazione sul trattamento che ha il maggiore impatto sull'interessato e su trattamenti che potrebbero coglierlo di sorpresa. Per i veicoli connessi l'EDPB raccomanda che l'interessato sia informato di tutti i destinatari attraverso le informazioni di primo livello. Come indicato dal Gruppo di lavoro Articolo 29 nelle linee guida sulla trasparenza, i titolari del trattamento dovrebbero fornire sui destinatari le informazioni più pregnanti per gli interessati. In pratica si tratterà solitamente dei nomi dei destinatari, in maniera tale che gli interessati sappiano con precisione chi è in possesso dei dati personali che li riguardano. Se i titolari del trattamento non sono in grado di fornire i nomi dei destinatari, le informazioni dovrebbero essere quanto più specifiche possibile e indicare la tipologia del destinatario (ad esempio facendo riferimento alle attività svolte), l'ambito di attività, il settore, il comparto e la sede dei destinatari.

88. Gli interessati possono essere informati mediante clausole concise e facilmente comprensibili contenute nel contratto di vendita del veicolo, oppure nel contratto di prestazione di servizi e/o in qualsiasi supporto scritto, utilizzando documenti distinti (ad esempio il manuale o il libretto di manutenzione del veicolo) oppure il computer di bordo.

89. In aggiunta alle informazioni necessarie si potrebbe fare ricorso a icone standardizzate, secondo quanto previsto dagli articoli 13 e 14 del GDPR, al fine di aumentare la trasparenza riducendo potenzialmente la necessità di presentare all'interessato grandi quantità di informazioni scritte. Le icone dovrebbero essere visibili nei veicoli così da fornire, in maniera comprensibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. L'EDPB sottolinea l'importanza di standardizzare le icone, affinché l'utente ritrovi gli stessi simboli indipendentemente dalla marca o dal modello del veicolo. Ad esempio quando sono raccolte determinate tipologie di dati, come dati relativi all'ubicazione, i veicoli potrebbero essere dotati di una segnalazione a bordo (ad esempio una spia all'interno del veicolo) che informi i passeggeri della raccolta di dati.

2.6 DIRITTI DELL'INTERESSATO

90. I produttori di veicoli e accessori, i fornitori di servizi e altri titolari del trattamento dovrebbero agevolare il controllo da parte degli interessati sui dati che li riguardano durante l'intero periodo del trattamento, attraverso strumenti specifici che consentano agli interessati di esercitare efficacemente i loro diritti, in particolare il diritto di accesso, di rettifica, di cancellazione, il diritto di limitazione di trattamento e, a seconda della base giuridica del trattamento, il diritto alla portabilità dei dati e il diritto di opposizione.

91. Per facilitare le modifiche delle impostazioni sarebbe opportuno attivare un sistema di gestione dei profili al fine di memorizzare le preferenze dei conducenti noti e aiutarli a modificare facilmente, in qualsiasi momento, le rispettive impostazioni sulla privacy. Il sistema di gestione dei profili dovrebbe centralizzare ogni impostazione dei dati per ciascun trattamento, soprattutto per facilitare l'accesso, la cancellazione, l'eliminazione e la portabilità dei dati personali provenienti dai sistemi del veicolo su richiesta dell'interessato. I conducenti dovrebbero avere la possibilità di bloccare temporaneamente o definitivamente, in qualsiasi momento, la raccolta di determinate tipologie di dati, salvo qualora il titolare del trattamento sia autorizzato a proseguire la raccolta di determinati dati sulla base di uno specifico fondamento giuridico. Nel caso di contratti che prevedono un'offerta personalizzata in base alla condotta di guida, ciò potrebbe comportare per l'utente il conseguente ripristino delle condizioni contrattuali standard. Tali funzionalità dovrebbero essere disponibili all'interno del veicolo ma potrebbero essere messe a disposizione degli interessati anche attraverso altri mezzi (ad esempio un'applicazione dedicata). Inoltre per consentire agli interessati di eliminare rapidamente e con facilità dati personali che possono essere memorizzati nel quadro strumenti della vettura (ad esempio cronologia della navigazione GPS, navigazione sul web ecc.) l'EDPB raccomanda ai costruttori di fornire una funzionalità semplice (ad esempio un pulsante di cancellazione).
92. Anche la vendita di un veicolo connesso e il conseguente passaggio di proprietà dovrebbero determinare la cancellazione di eventuali dati personali che non sono più necessari per le finalità specifiche precedenti, e l'interessato dovrebbe essere in grado di esercitare il suo diritto alla portabilità.

2.7 SICUREZZA

93. I produttori di veicoli e accessori, i fornitori di servizi e altri titolari del trattamento dovrebbero porre in essere misure atte a garantire la sicurezza e la riservatezza dei dati trattati e adottare tutte le precauzioni utili ad impedire che una persona non autorizzata acquisisca il controllo dei dati. In particolare gli operatori del settore dovrebbero prendere in considerazione l'adozione delle misure seguenti:

- cifratura dei canali di comunicazione per mezzo di un algoritmo conforme allo stato dell'arte;
- messa a punto di un sistema di gestione delle chiavi di cifratura che sia univoco per veicolo e non per modello;
- laddove i dati siano conservati a distanza, cifratura mediante algoritmi conformi allo stato dell'arte;
- aggiornamento periodico delle chiavi di cifratura;
- protezione delle chiavi di cifratura dalla possibile divulgazione;
- autenticazione dei dispositivi di ricezione di dati;
- misure atte a garantire l'integrità dei dati (ad esempio mediante *hashing*);

- tecniche di autenticazione utente affidabili per l'accesso ai dati personali (password, certificato elettronico ecc.).

94. Per quanto riguarda, più specificamente, le case costruttrici, l'EDPB raccomanda di attuare le misure di sicurezza seguenti:

- separazione delle funzioni vitali del veicolo da quelle che si basano costantemente sulle capacità di telecomunicazione (ad esempio "*infotainment*");
- attuazione di misure tecniche che consentano alle case costruttrici di correggere rapidamente le vulnerabilità di sicurezza durante la vita utile del veicolo;
- per quanto riguarda le funzioni vitali del veicolo, utilizzo prioritario, nei limiti del possibile, di mezzi di comunicazione sicuri specificamente dedicati al trasporto;
- creazione di un sistema di allarme in caso di attacco ai sistemi del veicolo, con la possibilità di attivare l'esercizio in modalità degradata[47];
- conservazione della cronologia degli accessi al sistema informatico del veicolo, ad esempio limitata ai sei mesi precedenti, per consentire di individuare l'origine di un potenziale attacco e di eseguire periodicamente un esame delle informazioni registrate in modo da individuare eventuali anomalie.

95. Queste raccomandazioni generali dovrebbero essere integrate da requisiti specifici che tengano conto delle caratteristiche e della finalità di ciascun trattamento.

2.8 TRASFERIMENTO DI DATI PERSONALI A TERZI

96. In linea di massima soltanto il titolare del trattamento e l'interessato hanno accesso ai dati generati da un veicolo connesso. Il titolare del trattamento può tuttavia trasmettere dati personali a un partner commerciale (destinatario), nella misura in cui tale trasmissione si fondi su una delle basi giuridiche di cui all'articolo 6 del GDPR.

97. Considerata la possibile sensibilità dei dati sull'uso del veicolo (ad esempio viaggi effettuati, stile di guida), l'EDPB raccomanda di ottenere sistematicamente il consenso dell'interessato prima di trasmettere i suoi dati a un partner commerciale che agisca in qualità di titolare del trattamento (ad esempio mediante la selezione di una casella non preselezionata oppure, ove tecnicamente fattibile, utilizzando un dispositivo fisico o logico a cui la persona possa accedere dal veicolo). Il partner commerciale diventa, a sua volta, responsabile dei dati che riceve ed è soggetto a tutte le disposizioni del GDPR.

98. Il produttore del veicolo, il fornitore di servizi o un altro titolare del trattamento può trasmettere dati personali a un responsabile del trattamento che interverrà nella prestazione del servizio all'interessato, fermo restando che il responsabile del trattamento non può utilizzare tali dati per i propri scopi. Titolari e responsabili del trattamento sono tenuti a redigere un contratto o un altro atto giuridico che specifichi gli obblighi di ciascuna parte e richiami le disposizioni dell'articolo 28 del GDPR.

2.9 TRASFERIMENTO DI DATI PERSONALI AL DI FUORI DELL'UE/DEL SEE

99. Quando i dati personali sono trasferiti al di fuori dello Spazio economico europeo sono previste speciali garanzie per assicurare che il trasferimento avvenga in condizioni di sicurezza.

100. Di conseguenza il titolare del trattamento può trasferire dati personali a un destinatario soltanto nella misura in cui tale trasferimento abbia luogo in conformità con i requisiti di cui al capo V del GDPR.

2.10 USO DI TECNOLOGIE WI-FI DI BORDO

101. I progressi compiuti nel campo della tecnologia cellulare hanno reso possibile l'utilizzo agevole di internet in viaggio. Oltre alla connettività Wi-Fi disponibile nel veicolo attraverso l'hotspot di uno smartphone o un dispositivo dedicato (dongle [chiave meccanica] OBD-II, router o modem wireless ecc.), oggi la maggioranza delle case produttrici offre modelli che includono una connessione dati cellulare integrata e sono anche in grado di creare reti Wi-Fi. A seconda dei casi si dovranno prendere in considerazione vari aspetti:

- la connettività Wi-Fi è offerta come servizio da un operatore del trasporto stradale, ad esempio da un tassista ai suoi clienti. In questo caso il professionista o la sua azienda potrebbe essere considerato un fornitore di servizi internet (ISP) e come tale essere soggetto a particolari obblighi e restrizioni riguardo al trattamento dei dati personali dei suoi clienti;
- la connettività Wi-Fi è ad uso esclusivo del conducente (non è disponibile per i passeggeri). In tal caso il trattamento dei dati personali è considerato un'attività a carattere esclusivamente personale o domestico ai sensi dell'articolo 2, paragrafo 2, lettera c), e del considerando 18 del GDPR.

102. In generale il proliferare di interfacce di connessione a internet tramite Wi-Fi presenta maggiori rischi per la tutela della vita privata delle persone. In effetti attraverso i loro veicoli gli utenti diventano emittenti continui e possono pertanto essere identificati e localizzati. Al fine di impedire la localizzazione i produttori di veicoli e accessori dovrebbero quindi predisporre opzioni "*opt-out*" di facile utilizzo atte a impedire il rilevamento dell'identificativo del servizio di rete (Service Set Identifier o SSID) della rete Wi-Fi di bordo.

3. STUDI DI CASI

103. La presente sezione illustra cinque esempi specifici di trattamento nel contesto dei veicoli connessi, corrispondenti ad altrettanti scenari che potrebbero configurarsi per le parti interessate del settore. Gli esempi riguardano trattamenti che richiedono una potenza di calcolo non erogabile localmente nel veicolo e/o il trasferimento di dati personali a un soggetto

terzo per l'esecuzione di un'ulteriore analisi o la fornitura di ulteriori funzionalità a distanza. Per ciascuna tipologia di trattamento si specificano le finalità previste, le categorie di dati raccolti, il periodo di conservazione di tali dati, i diritti degli interessati, le misure di sicurezza da attuare e i destinatari delle informazioni. Qualora alcuni di questi aspetti non siano illustrati nel prosieguo del documento, valgono le raccomandazioni generali formulate nelle sezioni precedenti.

104. Gli esempi prescelti non sono esaustivi e intendono fornire un'indicazione della varietà di tipologie di trattamento, di basi giuridiche, di soggetti ecc. che possono intervenire nel contesto dei veicoli connessi.

3.1 PRESTAZIONE DI UN SERVIZIO DA PARTE DI UN TERZO

105. Gli interessati possono stipulare un contratto con un fornitore di servizi per ricevere servizi a valore aggiunto relativi al proprio veicolo. Ad esempio l'interessato potrebbe stipulare una polizza di assicurazione basata sull'uso che preveda uno sconto del premio assicurativo in funzione del chilometraggio percorso ("Pay As You Drive") o della buona condotta di guida ("Pay How You Drive") e che richieda il monitoraggio delle abitudini di guida da parte dell'impresa di assicurazione. L'interessato potrebbe anche stipulare con una società un contratto che offra assistenza stradale in caso di guasto e che comporti la comunicazione della posizione del veicolo alla società, oppure con un fornitore di servizi per la ricezione di messaggi o avvisi relativi al funzionamento del veicolo (ad esempio avvisi sullo stato di usura dei freni o avvisi di manutenzione).

3.1.1 ASSICURAZIONE BASATA SULL'USO DEL VEICOLO

106. L'assicurazione "Pay as You Drive" è una tipologia di assicurazione basata sull'uso del veicolo che tiene traccia del chilometraggio percorso dal conducente e/o delle sue abitudini di guida per differenziare e ricompensare i conducenti che guidano in condizioni di "sicurezza" offrendo loro tariffe di premio scontate. L'assicuratore inviterà il conducente a installare un servizio telematico integrato, un'applicazione mobile o ad attivare un modulo integrato dal costruttore che tiene traccia dei chilometri percorsi e/o della condotta di guida (frenate, accelerazione rapida ecc.) del contraente. Le informazioni raccolte dal dispositivo telematico saranno utilizzate per assegnare al conducente un punteggio al fine di esaminare quali rischi potrebbe presentare per l'impresa di assicurazione.

107. Poiché l'assicurazione basata sull'uso del veicolo esige il consenso a norma dell'articolo 5, paragrafo 3, della direttiva e-privacy, l'EDPB sottolinea che il contraente deve avere la possibilità di scegliere una polizza di assicurazione non basata sull'uso. Se così non fosse il consenso non sarebbe considerato liberamente prestato, giacché l'esecuzione del contratto sarebbe condizionata alla prestazione del consenso. Inoltre l'articolo 7, pa-

ragrafo 3, del GDPR stabilisce che l'interessato ha il diritto di revocare il consenso.

3.1.1.1 Base giuridica

108. Quando i dati sono raccolti attraverso un servizio di comunicazione elettronica accessibile al pubblico (ad esempio attraverso la scheda SIM contenuta nel dispositivo telematico), sarà necessario ottenere il consenso per potere accedere a informazioni già archiviate nel veicolo come previsto dall'articolo 5, paragrafo 3, della direttiva e-privacy. In questo contesto, infatti, non è applicabile nessuna delle deroghe previste dalle suddette disposizioni: il trattamento non è eseguito al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica né riguarda un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente. Il consenso potrebbe essere ottenuto al momento della conclusione del contratto.

109. Per quanto riguarda il trattamento di dati personali successivo alla registrazione sull'apparecchiatura terminale dell'utente finale o all'accesso alla stessa, l'impresa di assicurazione può invocare l'articolo 6, paragrafo 1, lettera b), del GDPR in questo specifico contesto, a condizione che sia in grado di stabilire che il trattamento ha luogo nell'ambito di un contratto validamente concluso con l'interessato e che è necessario all'esecuzione di tale contratto. Nella misura in cui il trattamento è oggettivamente necessario per l'esecuzione del contratto concluso con l'interessato, l'EDPB ritiene che l'applicazione dell'articolo 6, paragrafo 1, lettera b), del GDPR non avrebbe per effetto di ridurre la tutela ulteriore offerta dall'articolo 5, paragrafo 3, della direttiva e-privacy in questo caso specifico. Tale fondamento giuridico si configura attraverso la stipula, da parte dell'interessato, del contratto con l'impresa di assicurazione.

3.1.1.2 Dati raccolti

110. I dati personali di cui tenere conto sono di due tipi:

- **dati commerciali e dati relativi alle operazioni**: informazioni di identificazione dell'interessato, dati relativi alle operazioni, dati relativi ai mezzi di pagamento ecc.;
- **dati di utilizzo**: dati personali generati dal veicolo, abitudini di guida, posizione ecc.

111. L'EDPB raccomanda che, nella misura del possibile e considerato il rischio che i dati raccolti tramite la *telematic box* possano essere utilizzati impropriamente per creare un profilo esatto degli spostamenti del conducente, i dati grezzi relativi alla condotta di guida siano trattati:

- all'interno del veicolo nelle *telematic box* o nello smartphone dell'utente, in modo tale che l'assicuratore abbia accesso soltanto ai dati dei risultati (ad

esempio un punteggio relativo alle abitudini di guida) e non ai dati grezzi dettagliati (cfr. la sezione 2.1);

- oppure dal fornitore di servizi telematici per conto del titolare del trattamento (l'impresa di assicurazione) per generare punteggi numerici che saranno trasferiti all'impresa di assicurazione con una frequenza prestabilita. In questo caso i dati grezzi devono essere separati dai dati direttamente riferiti all'identità del conducente. Ciò significa che il fornitore di servizi telematici riceve i dati in tempo reale ma ignora i nomi, le targhe e altre informazioni dei contraenti. Dall'altro lato l'assicuratore conosce i nomi dei contraenti ma riceve soltanto i punteggi e il chilometraggio totale e non i dati grezzi utilizzati per calcolare detti punteggi.

112. Occorre inoltre rilevare che laddove i soli dati necessari per l'esecuzione del contratto siano quelli relativi al chilometraggio, i dati relativi all'ubicazione non devono essere raccolti.

3.1.1.3 Periodo di conservazione

113. Nel contesto del trattamento di dati effettuato per l'esecuzione di un contratto (ossia per la prestazione di un servizio) è importante distinguere due tipologie di dati prima di definirne i rispettivi periodi di conservazione:

- **dati commerciali e dati relativi alle operazioni**: questi dati possono essere conservati in una banca dati attiva per l'intera durata del contratto. Al termine del contratto possono essere archiviati fisicamente (su un supporto distinto, ad esempio DVD) o logicamente (tramite gestione delle autorizzazioni) nell'eventualità di un contenzioso. Successivamente, una volta scaduti i termini legali di prescrizione, i dati devono essere cancellati o resi anonimi;
- **dati di utilizzo**: i dati di utilizzo possono essere classificati come dati grezzi o come dati aggregati. Come indicato sopra, laddove possibile, i titolari o i responsabili del trattamento non dovrebbero trattare dati grezzi. Se invece il trattamento è necessario, i dati grezzi dovrebbero essere conservati soltanto finché sono necessari all'elaborazione dei dati aggregati e alla verifica della validità del processo di aggregazione. I dati aggregati dovrebbero essere conservati soltanto per il periodo di tempo necessario alla prestazione del servizio o secondo quanto altrimenti previsto dal diritto dell'Unione o degli Stati membri.

3.1.1.4 Informazione e diritti degli interessati

114. Prima del trattamento di dati personali è necessario fornire all'interessato, in maniera trasparente e comprensibile, le informazioni di cui all'articolo 13 del GDPR. In particolare occorre fornire informazioni riguardanti il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo. In quest'ultimo caso l'EDPB

raccomanda di adottare un approccio di tipo esplicativo per evidenziare la differenza tra i dati grezzi e il punteggio ottenuto sulla base di tali dati, sottolineando, se del caso, che l'impresa di assicurazione provvederà a raccogliere unicamente il punteggio risultante ove appropriato.

115. Laddove i dati siano trattati non all'interno del veicolo ma da parte di un fornitore di servizi telematici per conto del titolare del trattamento (l'impresa di assicurazione), sarebbe utile informare l'interessato che, in questo caso, il fornitore non avrà accesso ai dati direttamente riferiti all'identità del conducente (quali nomi, targhe ecc.). Inoltre, considerata l'importanza di informare gli interessati in merito alle conseguenze del trattamento dei dati personali che li riguardano e dato che gli interessati non dovrebbero essere colti di sorpresa dal trattamento dei loro dati personali, l'EDPB raccomanda di informare l'interessato dell'esistenza della profilazione e delle relative conseguenze anche qualora la profilazione non comporti il processo decisionale automatizzato previsto all'articolo 22 del GDPR.

116. Per quanto riguarda i diritti degli interessati, questi devono essere informati specificamente dei mezzi di cui dispongono per esercitare il diritto di accesso, rettifica, limitazione e cancellazione. Poiché i dati grezzi raccolti in questo contesto sono forniti dall'interessato (tramite moduli specifici o attraverso la sua attività) e trattati sulla base dell'articolo 6, paragrafo 1, lettera b), del GDPR (esecuzione di un contratto), l'interessato ha la facoltà di esercitare il suo diritto alla portabilità dei dati. Come evidenziato nelle linee guida sul diritto alla portabilità dei dati, l'EDPB raccomanda fortemente ai titolari di "*spiegare con chiarezza la differenza fra le categorie di dati che un interessato può ricevere attraverso l'esercizio del diritto alla portabilità anziché del diritto di accesso*"[48].

117. Le informazioni possono essere fornite all'atto della sottoscrizione del contratto.

3.1.1.5 Destinatario

118. L'EDPB raccomanda che, nei limiti del possibile, i dati relativi all'utilizzo del veicolo siano trattati direttamente all'interno delle *telematic box*, affinché l'assicuratore abbia accesso unicamente ai dati dei risultati (ad esempio un punteggio) e non ai dati grezzi dettagliati.

119. Qualora i dati siano raccolti da un fornitore di servizi telematici per conto del titolare del trattamento (l'impresa di assicurazione) per generare punteggi numerici, il fornitore non avrà bisogno di conoscere l'identità del conducente (ad esempio nomi, targhe ecc.) o dei contraenti.

3.1.1.6 Sicurezza

120. Valgono le raccomandazioni generali. Cfr. la sezione 2.7.

3.1.2 AFFITTO E PRENOTAZIONE DI UN POSTO AUTO

121. Il proprietario di un posto auto decide di affittarlo. A tale scopo inserisce un annuncio e fissa il prezzo del posto auto su un'applicazione web. A inserimento effettuato, l'applicazione avvisa il proprietario ogni qual volta un conducente desideri prenotare il posto auto. Il conducente può scegliere una destinazione e verificare la disponibilità di parcheggi sulla base di una molteplicità di criteri. Ottenuta l'approvazione del proprietario, l'operazione è confermata e il fornitore del servizio tratta il pagamento e poi utilizza la navigazione per guidare l'utente fino a destinazione.

3.1.2.1 Base giuridica

122. Quando i dati sono raccolti per mezzo di una comunicazione elettronica accessibile al pubblico si applica l'articolo 5, paragrafo 3, della direttiva e-privacy.

123. Trattandosi di un servizio della società dell'informazione, l'articolo 5, paragrafo 3, della direttiva e-privacy non richiede l'ottenimento del consenso per poter accedere alle informazioni già archiviate nel veicolo qualora tale servizio sia esplicitamente richiesto dall'abbonato.

124. Per il trattamento di dati personali ed esclusivamente per i dati necessari all'esecuzione del contratto di cui l'interessato è parte la base giuridica sarà costituita dall'articolo 6, paragrafo 1, lettera b), del GDPR.

3.1.2.2 Dati raccolti

125. I dati trattati comprendono i dati di contatto del conducente (nome, e-mail, recapito telefonico), il tipo di veicolo (ad esempio autovettura, autocarro, motociclo), il numero di targa, il periodo di sosta, gli estremi del pagamento (ad esempio dati della carta di credito) nonché i dati di navigazione.

3.1.2.3 Periodo di conservazione

126. I dati dovrebbero essere conservati finché sono necessari all'esecuzione del contratto di parcheggio o secondo quanto altrimenti previsto dal diritto dell'Unione o degli Stati membri. Al termine di tale periodo i dati sono cancellati o resi anonimi.

3.1.2.4 Informazione e diritti degli interessati

127. Prima del trattamento di dati personali si dovrebbero fornire all'interessato, in maniera trasparente e comprensibile, le informazioni di cui all'articolo 13 del GDPR.

128. L'interessato dovrebbe essere informato specificamente dei mezzi di cui dispone per esercitare il diritto di accesso, rettifica, limitazione e cancellazione. Poiché i dati raccolti in questo contesto sono forniti dall'interessato (tramite moduli specifici o attraverso la sua attività) e trattati sulla base dell'articolo 6, paragrafo 1, lettera b), del GDPR (esecuzione di un contratto), l'interessato ha la facoltà di esercitare il suo diritto alla portabilità dei dati. Come evidenziato nelle linee guida sul diritto alla portabilità dei dati, l'EDPB raccomanda vivamente ai titolari di "*spiegare con chiarezza la differenza fra le categorie di dati che un interessato può ricevere attraverso l'esercizio del diritto alla portabilità anziché del diritto di accesso*".

3.1.2.5 Destinatario

129. In linea di massima soltanto il titolare e il responsabile del trattamento hanno accesso ai dati.

3.1.2.6 Sicurezza

130. Valgono le raccomandazioni generali. Cfr. la sezione 2.7.

3.2 eCALL

131. Nel caso di un incidente grave nell'Unione europea, il veicolo attiva automaticamente una chiamata eCall al numero 112, il numero di emergenza valido per tutta l'UE (per maggiori dettagli, cfr. la sezione 1.1) che consente l'invio tempestivo di un'ambulanza nel luogo dell'incidente a norma del regolamento (UE) 2015/758, del 29 aprile 2015, relativo ai requisiti di omologazione per lo sviluppo del sistema eCall di bordo basato sul servizio 112 e che modifica la direttiva 2007/46/CE (di seguito "regolamento (UE) 2015/758").

132. In effetti il generatore eCall installato all'interno del veicolo, che consente la trasmissione tramite una rete mobile di comunicazione senza fili, avvia una chiamata di emergenza, che è attivata automaticamente da sensori di bordo o manualmente dagli occupanti del veicolo soltanto in caso di incidente. Oltre all'attivazione del canale audio, il secondo evento attivato in automatico a seguito di un incidente consiste nel generare la serie minima di dati (Minimum Set of Data - MSD) e nel trasmetterla al centro di raccolta delle chiamate di emergenza (PSAP).

3.2.1 BASE GIURIDICA

133. Per quanto riguarda l'applicazione della direttiva e-privacy, occorre prendere in considerazione due disposizioni:

- l'articolo 9 riguardante i dati relativi all'ubicazione diversi dai dati relativi al traffico, che si applica soltanto ai servizi di comunicazione elettronica;
- l'articolo 5, paragrafo 3, per l'accesso alle informazioni archiviate nel generatore installato all'interno del veicolo.

134. Sebbene, in linea di massima, dette disposizioni prevedano il consenso dell'interessato, il regolamento (UE) 2015/758 costituisce un obbligo legale a cui il titolare del trattamento è soggetto (l'interessato non è in grado di operare una scelta autenticamente libera e sarà nell'impossibilità di rifiutare il trattamento dei dati che lo riguardano). Pertanto il regolamento (UE) 2015/758 prevale sulla necessità di ottenere il consenso del conducente per il trattamento dei dati relativi all'ubicazione e dell'MSD[49].

135. La base giuridica del trattamento di tali dati sarà l'adempimento di un obbligo legale come previsto dall'articolo 6, paragrafo 1, lettera c), del GDPR (ossia il regolamento (UE) 2015/758).

3.2.2 DATI RACCOLTI

136. Il regolamento (UE) 2015/758 stabilisce che i dati inviati dal sistema eCall di bordo basato sul 112 contengono solo le informazioni minime di cui alla norma EN 15722:2015 "Sistemi intelligenti di trasporto — eSafety — serie minima di dati per chiamate eCall (MSD)", ossia:

- l'indicazione dell'attivazione manuale o automatica della chiamata eCall;
- il tipo di veicolo;
- il numero di identificazione del veicolo (VIN);
- il tipo di propulsione del veicolo;
- la marcatura temporale del messaggio di dati iniziale generato nell'ambito dell'evento eCall in corso;
- le ultime coordinate di latitudine e longitudine note del veicolo, determinate il più tardi possibile prima che sia generato il messaggio;
- l'ultima direzione di marcia reale nota del veicolo, determinata il più tardi possibile prima che sia generato il messaggio (soltanto le ultime tre posizioni del veicolo).

3.2.3 PERIODO DI CONSERVAZIONE

137. Il regolamento (UE) 2015/758 stabilisce che i dati sono conservati solo per il periodo di tempo necessario ad affrontare le situazioni di emergenza. Tali dati sono cancellati completamente quando non sono più necessari per tale scopo. Inoltre i dati sono soppressi automaticamente e costantemente dalla memoria interna del sistema eCall. È possibile conservare soltanto le ultime tre posizioni del veicolo nella misura in cui ciò risulti strettamente necessario a indicare la posizione attuale e la direzione di marcia del veicolo al momento dell'evento.

3.2.4 INFORMAZIONE E DIRITTI DEGLI INTERESSATI

138. A norma dell'articolo 6 del regolamento (UE) 2015/758 i costruttori devono fornire informazioni chiare e complete sul trattamento dei dati effettuato attraverso il sistema eCall. Le informazioni sono fornite nel manuale di istruzioni del proprietario separatamente per il sistema eCall di bordo basato sul 112 e per eventuali sistemi eCall supportati da servizi di terzi prima dell'utilizzo del sistema. Le informazioni includono:

- il riferimento alla base giuridica per il trattamento;
- la precisazione del fatto che il sistema eCall di bordo basato sul 112 è attivato in automatico;
- le modalità del trattamento di dati svolto dal sistema eCall di bordo basato sul 112;
- le finalità specifiche del trattamento di dati di eCall, che è limitato alle situazioni di emergenza di cui all'articolo 5, paragrafo 2, primo comma, del regolamento (UE) 2015/758;
- i tipi di dati raccolti ed elaborati e i destinatari di tali dati;
- il periodo di conservazione dei dati nel sistema eCall di bordo basato sul 112;
- la precisazione del fatto che non vi è alcun tracciamento costante del veicolo;
- le modalità per l'esercizio dei diritti degli interessati nonché il servizio di contatto responsabile della gestione delle domande di accesso;
- eventuali informazioni supplementari necessarie riguardo alla tracciabilità, al controllo e al trattamento dei dati personali in relazione alla fornitura di un sistema eCall supportato da servizi di terzi (TPS eCall) e/o di altri servizi a valore aggiunto, che sono soggetti al consenso esplicito del proprietario e conformi al GDPR. Occorre tenere conto in modo particolare del fatto che possono esistere differenze tra il trattamento dei dati eseguito mediante il sistema eCall di bordo basato sul 112 e i sistemi TPS eCall di bordo o altri servizi a valore aggiunto.

139. Inoltre anche il fornitore di servizi deve fornire agli interessati, in maniera trasparente e comprensibile, le informazioni di cui all'articolo 13 del GDPR. In particolare l'interessato deve essere informato delle finalità del trattamento cui sono destinati i dati personali, nonché del fatto che il trattamento dei dati personali si basa su un obbligo legale a cui è soggetto il titolare del trattamento.

140. Tenendo conto della natura del trattamento, le informazioni sui destinatari o sulle categorie di destinatari dei dati personali dovrebbero essere chiare e gli interessati dovrebbero essere informati del fatto che i dati non sono disponibili ad alcun soggetto al di fuori del sistema eCall di bordo basato sul 112 prima dell'attivazione del sistema eCall.

141. Per quanto riguarda i diritti degli interessati, occorre rilevare che, poiché il trattamento è basato su un obbligo legale, il diritto di opposizione e il diritto alla portabilità non si applicano.

3.2.5 DESTINATARIO

142. I dati non sono disponibili ad alcun soggetto al di fuori del sistema eCall di bordo basato sul 112 prima dell'attivazione del sistema eCall.

143. Una volta attivato (manualmente dagli occupanti del veicolo o automaticamente non appena un sensore di bordo rileva una collisione grave), il sistema eCall stabilisce una connessione vocale con lo PSAP pertinente e l'MSD è inviato all'operatore dello PSAP.

144. Inoltre i dati trasmessi attraverso il sistema eCall di bordo basato sul 112 e trattati dagli PSAP possono essere trasferiti ai servizi di pronto intervento e ai servizi associati di cui alla decisione n. 585/2014/UE solo in caso di incidenti relativi a eCall e alle condizioni di cui alla stessa decisione; tali dati sono utilizzati esclusivamente al fine di conseguire gli obiettivi di cui alla suddetta decisione. I dati trattati dagli PSAP attraverso il sistema eCall di bordo basato sul 112 non sono trasmessi ad alcuna parte terza senza il previo consenso esplicito dell'interessato.

3.2.6 SICUREZZA

145. Il regolamento (UE) 2015/758 stabilisce che nel sistema eCall devono essere integrate tecnologie atte a rafforzare la tutela della privacy, al fine di fornire agli utenti un livello di protezione adeguato, nonché le necessarie tutele per prevenire attività di sorveglianza e abusi. Inoltre le case costruttrici dovrebbero garantire che il sistema eCall basato sul numero 112 e qualunque altro sistema che fornisca un servizio eCall gestito da servizi di terzi o un servizio a valore aggiunto siano progettati in modo da non consentire lo scambio di dati personali tra tali sistemi.

146. Per quanto riguarda gli PSAP, gli Stati membri dovrebbero assicurarsi che i dati personali siano protetti dagli abusi, compresi la perdita oppure l'accesso e la modifica non autorizzati, e che siano definiti a livello adeguato e debitamente rispettati protocolli in materia di memorizzazione, periodo di conservazione, trattamento e protezione.

3.3 STUDI SULL'INCIDENTALITÀ

147. Gli interessati possono partecipare, su base volontaria, a studi sull'incidentalità finalizzati ad approfondire la conoscenza delle cause degli incidenti stradali e, più in generale, a perseguire finalità scientifiche.

3.3.1 BASE GIURIDICA

148. Quando i dati sono raccolti attraverso un servizio pubblico di comunicazione elettronica, il titolare del trattamento dovrà ottenere il consenso

dell'interessato per poter accedere a informazioni già archiviate nel veicolo come previsto dall'articolo 5, paragrafo 3, della direttiva e-privacy. In questo contesto, infatti, non è applicabile nessuna delle deroghe previste dalle suddette disposizioni: il trattamento non è eseguito al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica né riguarda un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente.

149. Per quanto riguarda il trattamento di dati personali e tenendo conto della varietà e della quantità dei dati personali necessari per gli studi sull'incidentalità, l'EDPB raccomanda che il trattamento sia basato sul previo consenso dell'interessato conformemente all'articolo 6 del GDPR. Tale consenso previo deve essere espresso in una forma specifica, attraverso la quale l'interessato manifesti la volontà di partecipare allo studio e acconsenta al trattamento dei suoi dati personali per tale finalità. Il consenso deve essere un'espressione di volontà libera, specifica e informata della persona i cui dati sono trattati (ad esempio selezione di una casella non preselezionata o configurazione del computer di bordo per attivare una funzione nel veicolo). Tale consenso deve essere prestato separatamente, per finalità specifiche e non può essere accorpato al contratto di acquisto o leasing di una nuova autovettura; inoltre deve poter essere revocato con la stessa facilità con cui lo si è espresso. La revoca del consenso determina l'interruzione del trattamento e la conseguente cancellazione dei dati dalla banca dati attiva o l'anonimizzazione degli stessi.

150. Il consenso richiesto a norma dell'articolo 5, paragrafo 3, della direttiva e-privacy e il consenso necessario come fondamento giuridico per il trattamento dei dati possono essere ottenuti nello stesso momento (ad esempio mediante la selezione di una casella che indichi con chiarezza l'oggetto del consenso espresso dall'interessato).

151. Occorre rilevare che, in base alle condizioni del trattamento (natura del titolare del trattamento ecc.), si potrà individuare legittimamente un'altra base giuridica, purché questa non riduca l'ulteriore tutela offerta dall'articolo 5, paragrafo 3, della direttiva e-privacy (cfr. il punto 15). Qualora il trattamento sia basato su un altro fondamento giuridico come ad esempio l'esecuzione di un compito di interesse pubblico (articolo 6, paragrafo 1, lettera e), del GDPR), l'EDPB raccomanda di includere nello studio gli interessati su base volontaria.

3.3.2 DATI RACCOLTI

152. Il titolare del trattamento raccoglie dati personali strettamente necessari al trattamento.

153. Occorre prendere in considerazione due tipologie di dati:

- **dati relativi ai partecipanti e ai veicoli;**
- **dati tecnici provenienti dai veicoli** (velocità istantanea ecc.).

154. Gli studi scientifici nel campo dell'incidentalità giustificano la raccolta di dati relativi alla velocità istantanea, anche da parte di persone giuridiche che non gestiscono un servizio pubblico in senso stretto.

155. In effetti, come rilevato sopra, l'EDPB ritiene che i dati relativi alla velocità istantanea raccolti nell'ambito di uno studio sull'incidentalità non costituiscano dati relativi a reati per via della destinazione d'uso (ossia non sono raccolti a fini di indagine o perseguimento di un reato), il che ne giustifica la raccolta da parte di persone giuridiche che non gestiscono un servizio pubblico in senso stretto.

3.3.3 PERIODO DI CONSERVAZIONE

156. È importante distinguere due tipologie di dati. In primo luogo i dati relativi ai partecipanti e ai veicoli, che possono essere conservati per tutta la durata dello studio. In secondo luogo i dati tecnici provenienti dai veicoli, che dovrebbero essere conservati per il periodo più breve possibile per il conseguimento della specifica finalità. A tale riguardo, cinque anni dalla data di conclusione dello studio rappresentano un periodo ragionevole. Al termine di tale periodo i dati devono essere cancellati o resi anonimi.

3.3.4 INFORMAZIONE E DIRITTI DEGLI INTERESSATI

157. Prima del trattamento di dati personali è necessario fornire all'interessato, in maniera trasparente e comprensibile, le informazioni di cui all'articolo 13 del GDPR. In particolare, in caso di raccolta di dati relativi alla velocità istantanea, gli interessati dovrebbero essere informati specificamente di tale raccolta. Poiché il trattamento di dati è basato sul consenso, l'interessato deve essere informato specificamente dell'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basato sul consenso prestato prima della revoca. Inoltre poiché i dati raccolti in tale contesto sono forniti dall'interessato (tramite moduli specifici o attraverso la sua attività) e trattati sulla base dell'articolo 6, paragrafo 1, lettera a), del GDPR (consenso), l'interessato ha la facoltà di esercitare il suo diritto alla portabilità dei dati. Come evidenziato nelle linee guida sul diritto alla portabilità dei dati, l'EDPB raccomanda vivamente ai titolari di "spiegare con chiarezza la differenza fra le categorie di dati che un interessato può ricevere attraverso l'esercizio del diritto alla portabilità anziché del diritto di accesso". Pertanto il titolare del trattamento dovrebbe offrire una modalità semplice per revocare il consenso, liberamente e in qualsiasi momento, e dovrebbe sviluppare strumenti che gli consentano di rispondere alle richieste di portabilità dei dati.

158. Tali informazioni possono essere fornite al momento della sottoscrizione del modulo con cui l'interessato accetta di partecipare allo studio sull'incidentalità.

3.3.5 DESTINATARIO

159. In linea di massima soltanto il titolare e il responsabile del trattamento hanno accesso ai dati.

3.3.6 SICUREZZA

160. Come rilevato sopra, le misure di sicurezza poste in essere devono essere adattate al livello di sensibilità dei dati. Se, ad esempio, lo studio sull'incidentalità comporta la raccolta di dati relativi alla velocità istantanea (o qualunque altro tipo di dati relativi a condanne penali e a reati), l'EDPB raccomanda vivamente di porre in essere misure di sicurezza efficaci, ad esempio:

- attuazione di misure di pseudonimizzazione (ad esempio hashing con chiave segreta di dati quali cognome/nome dell'interessato e numero di serie);
- conservazione dei dati relativi alla velocità istantanea e dei dati relativi all'ubicazione in banche dati separate (ad esempio utilizzando un meccanismo di cifratura conforme allo stato dell'arte con procedure di approvazione e chiavi distinte);
- e/o cancellazione dei dati relativi all'ubicazione non appena l'evento o la sequenza di riferimento siano stati qualificati (ad esempio: tipo di strada, evento diurno/notturno) e conservazione dei dati di identificazione diretta in un database separato a cui abbia accesso soltanto un ristretto numero di persone.

3.4 FURTO D'AUTO

161. In caso di furto gli interessati potrebbero voler tentare di ritrovare il proprio veicolo utilizzando la localizzazione. L'uso dei dati relativi all'ubicazione è strettamente limitato alle esigenze dell'indagine e alla valutazione del caso da parte delle autorità competenti.

3.4.1 BASE GIURIDICA

162. Quando i dati sono raccolti per mezzo di un servizio di comunicazione elettronica accessibile al pubblico si applica l'articolo 5, paragrafo 3, della direttiva e-privacy.

163. Trattandosi di un servizio della società dell'informazione, l'articolo 5, paragrafo 3, della direttiva e-privacy non richiede l'ottenimento del consenso per poter accedere alle informazioni già archiviate nel veicolo qualora tale servizio sia esplicitamente richiesto dall'abbonato.

164. Per quanto riguarda il trattamento di dati personali, il fondamento giuridico per il trattamento dei dati relativi all'ubicazione sarà il consenso del proprietario del veicolo o, se del caso, l'esecuzione di un contratto (soltanto per i dati necessari all'esecuzione del contratto di cui il proprietario del veicolo è parte).

165. Il consenso deve essere un'espressione di volontà libera, specifica e informata della persona i cui dati sono trattati (ad esempio selezione di una casella non preselezionata o configurazione del computer di bordo per attivare una funzione sul veicolo). La libertà di espressione del consenso comporta la possibilità di revocare il consenso in qualsiasi momento e l'interessato dovrebbe esserne informato espressamente. La revoca del consenso determina l'interruzione del trattamento. A questo punto i dati dovrebbero essere cancellati dalla banca dati attiva, resi anonimi oppure archiviati.

3.4.2 DATI RACCOLTI

166. I dati relativi all'ubicazione possono essere trasmessi soltanto a partire dalla denuncia del furto; per il resto, non possono essere raccolti su base continuativa.

3.4.3 PERIODO DI CONSERVAZIONE

167. I dati relativi all'ubicazione possono essere conservati esclusivamente per il periodo durante il quale il caso è oggetto di valutazione da parte delle autorità competenti, oppure fino al termine di una procedura di accertamento dei fatti che non si concluda con la conferma del furto del veicolo.

3.4.4 INFORMAZIONE DELL'INTERESSATO

168. Prima del trattamento di dati personali si dovrebbero fornire all'interessato, in maniera trasparente e comprensibile, le informazioni di cui all'articolo 13 del GDPR. Più specificamente l'EDPB raccomanda che il titolare del trattamento evidenzi che il veicolo non è sottoposto a sorveglianza costante e che i dati relativi all'ubicazione possono essere raccolti e trasmessi soltanto a partire dalla denuncia del furto. Inoltre il titolare del trattamento deve fornire all'interessato informazioni relative al fatto che l'accesso ai dati è consentito soltanto agli operatori autorizzati della piattaforma di telesorveglianza e alle autorità legalmente autorizzate.

169. Per quanto riguarda i diritti degli interessati, quando il trattamento dei dati è basato sul consenso l'interessato dovrebbe essere informato specificamente dell'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basato sul consenso prestato prima della revoca. Inoltre quando i dati raccolti in questo con-

testo sono forniti dall'interessato (tramite moduli specifici o attraverso la sua attività) e trattati sulla base dell'articolo 6, paragrafo 1, lettera a) (consenso), o dell'articolo 6, paragrafo 1, lettera b) (esecuzione di un contratto), del GDPR l'interessato ha la facoltà di esercitare il suo diritto alla portabilità dei dati. Come evidenziato nelle linee guida sul diritto alla portabilità dei dati, l'EDPB raccomanda vivamente ai titolari di "*spiegare con chiarezza la differenza fra le categorie di dati che un interessato può ricevere attraverso l'esercizio del diritto alla portabilità anziché del diritto di accesso*".

170. Pertanto il titolare del trattamento dovrebbe offrire una modalità semplice per revocare il consenso (solo laddove il consenso costituisca il fondamento giuridico del trattamento), liberamente e in qualsiasi momento, e dovrebbe sviluppare strumenti che gli consentano di rispondere alle richieste di portabilità dei dati.

171. Le informazioni possono essere fornite all'atto della sottoscrizione del contratto.

3.4.5 DESTINATARI

172. Nel caso di una denuncia di furto, i dati relativi all'ubicazione possono essere trasmessi i) agli operatori autorizzati della piattaforma di telesorveglianza e ii) alle autorità legalmente autorizzate.

3.4.6 SICUREZZA

173. Valgono le raccomandazioni generali. Cfr. la sezione 2.7.

NOTE

[1] I riferimenti agli "Stati membri" nel presente documento sono da intendersi come riferimenti agli "Stati membri del SEE".

[2] Infografica "Data and the connected car" del Future of Privacy Forum; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf.

[3] Campagna "My Car My Data", http://www.mycarmydata.eu/.

[4] The interoperable EU-wide eCall, https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en

[5] Decisione n. 585/2014/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, sulla diffusione in tutto il territorio dell'Unione europea di un servizio elettronico di chiamata di emergenza (eCall) interoperabile (Testo rilevante ai fini del SEE), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32014D0585

[6] Documento di lavoro sulle implicazioni in materia di protezione dei dati e rispetto della vita privata dell'iniziativa eCall, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_it.pdf

[7] Cyber security and resilience of smart cars", https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.

[8] "Resolution on data protection in automated and connected vehicles", https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf

[9] Documento di lavoro "Connected Vehicles", https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/

[10] "Data protection aspects of using connected and non-connected vehicles", https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf.

[11] Principles of cyber security for connected and automated vehicles, https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

[12] Pacchetto di conformità per un uso responsabile dei dati nelle automobili connesse, https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data

[13] Direttiva 2008/63/CE della Commissione, del 20 giugno 2008, relativa alla concorrenza sui mercati delle apparecchiature terminali di telecomunicazioni (Versione codificata) (Testo rilevante ai fini del SEE), https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX%3A32008L0063.

[14] Comitato europeo per la protezione dei dati, Parere 5/2019 sull'interazione tra la direttiva e-privacy e il regolamento generale sulla protezione dei dati, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati, adottato il 12 marzo 2019 (di seguito "parere 5/2019"), punto 40.

[15] Ibidem, punto 40.

[16] Ibidem, punto 41.

[17] Il consenso richiesto dall'articolo 5, paragrafo 3, della direttiva "e-privacy" e il consenso necessario come fondamento giuridico per il trattamento dei dati (articolo 6 del GDPR) per la medesima finalità specifica possono essere ottenuti nello stesso momento (ad esempio mediante la selezione di una casella che indichi con chiarezza l'oggetto del consenso espresso dall'interessato).

[18] Parere 5/2019, punto 41.

[19] Comitato europeo per la protezione dei dati, Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, Versione 2.0, 8 ottobre 2019, punto 1.

[20] PwC Strategy 2014. "In the fast lane. The bright future of connected cars", https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf.

[21] Cfr. l'articolo 2, paragrafo 2, lettera c), del GDPR.

[22] Il Gruppo di lavoro Articolo 29 si è espresso a tale riguardo nel parere 2/2017 sul trattamento dei dati sul posto di lavoro (WP249), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

[23] Per maggiori informazioni cfr. https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematical-

ly-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html

[24] Markus Ullmann, Tobias Franz, and Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier -- Analysis, and Measurements, in Proceedings, VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, France, July 23 to 27, 2017, pagg. 32-37.

[25] Direttiva 2010/40/UE del Parlamento europeo e del Consiglio, del 7 luglio 2010, sul quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto, https://eur-lex.europa.eu/legal-content/it/TXT/PDF/?uri=CELEX:32010L0040

[26] Gruppo di lavoro Articolo 29 - Parere 03/2017 sul documento intitolato "Trattamento dei dati personali nel contesto del sistema di trasporto intelligente cooperativo (C-ITS)", http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171.

[27] Cfr. l'articolo 4, punto 2, del GDPR.

[28] Cfr. l'articolo 4, punto 1, del GDPR.

[29] Cfr. l'articolo 4, punto 7, del GDPR e il documento del comitato europeo per la protezione dei dati dal titolo Guidelines 07/2020 on the concepts of controller and processor in the GDPR (di seguito "Linee guida 07/2020").

[30] Cfr. l'articolo 4, punto 8, del GDPR e le linee guida 07/2020.

[31] Cfr. l'articolo 4, punto 9, del GDPR e le linee guida 07/2020.

[32] Articolo 4, punto 9, e considerando 31 del GDPR.

[33] Gruppo di lavoro Articolo 29 – Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_it.pdf

[34] Comitato europeo per la protezione dei dati, Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, Versione 1.1, 4 maggio 2020 (di seguito "linee guida 5/2020").

[35] Cfr. anche comitato europeo per la protezione dei dati, Guidelines 10/2020 on restrictions under Article 23 GDPR.

[36] Linee guida 5/2020, sezioni 3.2 e 3.3.

[37] Il principio di divieto di cui all'articolo 9, paragrafo 1, del GDPR riguarda esclusivamente i *"dati biometrici intesi a identificare in modo univoco una persona fisica"*.

[38] Articolo 5, paragrafo 1, lettera c), del GDPR.

[39] Cfr. anche comitato europeo per la protezione dei dati, Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita, Versione 2.0, adottate il 20 ottobre 2020 (di seguito "linee guida 4/2019").

[40] Per ulteriori raccomandazioni in materia di tutela della vita privata fin dalla progettazione e per impostazione predefinita, cfr. anche le linee guida 4/2019.

[41] Gruppo di lavoro Articolo 29 – Parere 05/2012 sul cloud computing, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_it.pdf.

[42] Cfr. l'articolo 4, punto 1, e il considerando 26 del GDPR.

[43] Gruppo di lavoro Articolo 29 - Parere 05/2014 sulle tecniche di anonimizzazione, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf.

[44] Articolo 4, punto 5, del GDPR. Relazione dell'Enisa del 3 dicembre 2019, https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.

[45] Articolo 5, paragrafo 1, lettera a), e articolo 13 del GDPR. Cfr. anche il documento del Gruppo di lavoro Articolo 29 Linee guida sulla trasparenza ai sensi del regolamento 2016/679 (wp260rev.01), approvato dall'EDPB.

[46] Cfr. il documento del Gruppo di lavoro Articolo 29 Linee guida sulla trasparenza ai sensi del regolamento 2016/679 (wp260rev.01), approvato dall'EDPB.

[47] La modalità degradata è una modalità di esercizio che garantisce le funzioni essenziali per l'utilizzo in sicurezza del veicolo (ad esempio requisiti minimi di sicurezza), nonostante la disattivazione di altre funzionalità meno importanti (ad esempio il funzionamento del dispositivo di geoguida può essere considerato non essenziale, a differenza dell'impianto frenante).

[48] Gruppo di lavoro Articolo 29, Linee guida sul diritto alla "portabilità dei dati" (WP242) rev.01, approvate dall'EDPB, pag. 13.

[49] Occorre rilevare che l'articolo 8, paragrafo 1, lettera f), del mandato negoziale del Consiglio sulla proposta di regolamento "e-privacy" prevede effettivamente una deroga specifica per il sistema eCall in quanto il consenso non è richiesto *se è necessario localizzare l'apparecchiatura terminale quando un utente finale effettua una comunicazione di emergenza al numero unico di emergenza europeo "112" o al numero di emergenza nazionale, in conformità dell'articolo 13, paragrafo 3.*

Linee guida 06/2020 sull'interazione tra la seconda direttiva sui servizi di pagamento e il GDPR Versione 2.0

Adottate il 15 dicembre 2020

Cronologia delle versioni

Versione 2.0	15 dicembre 2020	Adozione delle linee guida a seguito della consultazione pubblica
Versione 1.0	17 luglio 2020	Adozione delle linee guida ai fini della consultazione per la pubblicazione

Indice

1 Introduzione
- 1.1 Definizioni
- 1.2 Servizi nell'ambito della PSD2

2 Fondamenti di liceità e ulteriore trattamento a norma della PSD2
- 2.1 Fondamenti di liceità del trattamento
- 2.2 Articolo 6, paragrafo 1, lettera b), del GDPR (il trattamento è necessario all'esecuzione di un contratto)
- 2.3 Prevenzione delle frodi
- 2.4 Ulteriore trattamento (AISP e PISP)
- 2.5 Motivo lecito per concedere l'accesso al conto (ASPSP)

3 Consenso esplicito
- 3.1 Consenso ai sensi del GDPR
- 3.2 Consenso ai sensi della PSD2
  - 3.2.1 Consenso esplicito ai sensi dell'articolo 94, paragrafo 2, della PSD2
- 3.3 Conclusioni

4 Trattamento dei dati dei taciti interessati
- 4.1 Dati dei taciti interessati
- 4.2 Interesse legittimo del titolare del trattamento
- 4.3 Ulteriore trattamento dei dati personali dei taciti interessati

5 Trattamento di categorie particolari di dati personali a norma della PSD2
- 5.1 Categorie particolari di dati personali
- 5.2 Deroghe possibili
- 5.3 Interesse pubblico rilevante
- 5.4 Consenso esplicito
- 5.5 Assenza di deroghe applicabili

6 Minimizzazione dei dati, sicurezza, trasparenza, responsabilizzazione e profilazione
- 6.1 Minimizzazione dei dati e protezione dei dati fin dalla progettazione e per impostazione predefinita
- 6.2 Misure di minimizzazione dei dati
- 6.3 Sicurezza
- 6.4 Trasparenza e responsabilizzazione
- 6.5 Profilazione

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI,

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati),

visto l'accordo sullo Spazio economico europeo (SEE), in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

visti gli articoli 12 e 22 del proprio regolamento interno,

considerando quanto segue:

(1) Il regolamento generale sulla protezione dei dati (di seguito "GDPR") prevede un insieme coerente di norme per il trattamento dei dati personali in tutta l'UE.

(2) La seconda direttiva sui servizi di pagamento (direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 dicembre 2015, di seguito "PSD2") abroga la direttiva 2007/64/CE e stabilisce nuove norme per garantire certezza giuridica ai consumatori, ai commercianti e alle imprese nella catena di pagamento e per modernizzare il quadro giuridico riguardante il mercato dei servizi di pagamento[2]. Gli Stati membri erano tenuti a recepire la PSD2 nei rispettivi ordinamenti nazionali entro il 13 gennaio 2018.

(3) Un elemento importante della PSD2 è l'introduzione di un quadro giuridico per i nuovi servizi di disposizione di ordine di pagamento e servizi di informazione sui conti. La PSD2 consente ai prestatori di questi nuovi servizi di pagamento di avere accesso ai conti di pagamento degli interessati ai fini della prestazione di detti servizi.

(4) Per quanto riguarda la protezione dei dati, a norma dell'articolo 94, paragrafo 1, della PSD2, qualsiasi trattamento di dati personali, compresa la fornitura di informazioni in merito al trattamento, ai fini della PSD2 deve essere effettuato in conformità del GDPR[3] e del regolamento (UE) 2018/1725.

(5) Il considerando 89 della PSD2 afferma che, qualora ai fini della direttiva vi sia trattamento di dati personali, è opportuno che sia specificato lo scopo preciso, siano citate le basi giuridiche pertinenti, vi sia conformità con i requisiti di sicurezza pertinenti di cui al GDPR e siano rispettati i principi di necessità, proporzionalità, limitazione delle finalità e proporzionalità del periodo di conservazione dei dati. Inoltre la protezione dei dati fin dalla progettazione e la protezione dei dati per impostazione predefinita dovrebbero essere integrate in tutti i sistemi di trattamento dei dati sviluppati e utilizzati nel quadro della PSD2[4].

(6) Il considerando 93 della PSD2 afferma che i prestatori di servizi di disposi-

zione di ordine di pagamento e i prestatori di servizi di informazione sui conti, da una parte, e il prestatore di servizi di pagamento di radicamento del conto, dall'altra, dovrebbero soddisfare i necessari requisiti in materia di protezione e sicurezza dei dati stabiliti o citati nella direttiva o indicati nei progetti di norme tecniche di regolamentazione,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

1. INTRODUZIONE

1. La seconda direttiva sui servizi di pagamento (di seguito "PSD2") ha introdotto una serie di novità nel settore dei servizi di pagamento. Pur creando nuove opportunità per i consumatori e aumentando la trasparenza in tale ambito, l'applicazione della PSD2 solleva alcune questioni e preoccupazioni riguardo alla necessità che gli interessati mantengano il pieno controllo dei loro dati personali. Il regolamento generale sulla protezione dei dati (di seguito "GDPR") si applica al trattamento dei dati personali, comprese le attività di trattamento effettuate nell'ambito di servizi di pagamento ai sensi della PSD2[5]. Pertanto i titolari del trattamento che operano nel settore disciplinato dalla PSD2 devono sempre garantire il rispetto dei requisiti del GDPR, compresi i principi di protezione dei dati di cui all'articolo 5 dello stesso, e delle pertinenti disposizioni della direttiva relativa alla vita privata e alle comunicazioni elettroniche[6]. Benché la PSD2[7] e le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (di seguito "norme tecniche di regolamentazione"[8]) contengano talune disposizioni relative alla protezione e alla sicurezza dei dati, sono emerse incertezze circa l'interpretazione di tali disposizioni e l'interazione tra il quadro generale in materia di protezione dei dati e la PSD2.
2. Il 5 luglio 2018 l'EDPB ha pubblicato una lettera relativa alla PSD2, nella quale ha fornito chiarimenti su questioni relative alla protezione dei dati personali in relazione alla PSD2, in particolare sul trattamento dei dati personali di soggetti diversi dai contraenti (i cosiddetti "*silent party data*", ossia i "dati dei taciti interessati") da parte dei prestatori di servizi di informazione sui conti (di seguito "AISP") e dei prestatori di servizi di disposizione di ordine di pagamento (di seguito "PISP"), sulle procedure relative alla prestazione e alla revoca del consenso, sulle norme tecniche di regolamentazione e sulla cooperazione tra i prestatori di servizi di pagamento di radicamento del conto (di seguito "ASPSP") in relazione alle misure di sicurezza. Al fine di individuare le sfide più urgenti da affrontare, nell'ambito dell'attività di formulazione delle presenti linee guida si è provveduto a raccogliere contributi delle parti interessate, sia per iscritto che in occasione di un evento dedicato ai portatori di interessi.
3. L'obiettivo delle presenti linee guida è fornire ulteriori orientamenti su aspetti relativi alla protezione dei dati nel contesto della PSD2, in particolare sulla relazione tra le pertinenti disposizioni del GDPR e della direttiva. Le presenti linee guida si concentrano principalmente sul trattamento dei dati personali da parte degli AISP e dei PISP. Di conseguenza il presente documento verte sulle condizioni necessarie affinché gli ASPSP possano concedere l'accesso alle informazioni sui conti di pagamento e affinché i PISP e gli AISP possano procedere al trattamento dei dati personali, compresi i requisiti e le garanzie vigenti in relazione al trattamento dei dati personali da parte dei PISP e degli AISP per fini diversi dalle finalità iniziali per le quali i dati sono stati raccolti, in particolare nel caso in cui siano stati raccolti nell'ambito della prestazione di un servizio di informazione sui conti[9]. Nel presente documento vengono discusse inoltre le diverse nozioni di consenso esplicito ai sensi della PSD2

e del GDPR, nonché il trattamento dei "dati dei taciti interessati", il trattamento di categorie particolari di dati personali da parte dei PISP e degli AISP, l'applicazione dei principi fondamentali di protezione dei dati stabiliti dal GDPR, tra cui la minimizzazione dei dati, la trasparenza, la responsabilizzazione e le misure di sicurezza. La PSD2 comporta responsabilità trasversali nei settori, tra l'altro, della protezione dei consumatori e del diritto in materia di concorrenza. Le considerazioni relative a tali ambiti del diritto esulano dall'oggetto delle presenti linee guida.

4. Per agevolare la lettura delle linee guida, si riportano di seguito le definizioni dei principali termini utilizzati nel presente documento.

1.1 DEFINIZIONI

"Prestatore di servizi di informazione sui conti" ("AISP"): il prestatore di un servizio online che fornisce informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento.

"Prestatore di servizi di pagamento di radicamento del conto" ("ASPSP"): un prestatore di servizi di pagamento che fornisce e amministra un conto di pagamento per un pagatore.

"Minimizzazione dei dati": un principio di protezione dei dati in base al quale i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

"Pagatore": una persona fisica o giuridica detentrice di un conto di pagamento che autorizza l'ordine di pagamento a partire da detto conto di pagamento o, in mancanza di conto di pagamento, una persona fisica o giuridica che dà l'ordine di pagamento.

"Beneficiario": una persona fisica o giuridica che è il destinatario previsto dei fondi che sono stati oggetto di un'operazione di pagamento.

"Conto di pagamento": un conto detenuto a nome di uno o più utilizzatori di servizi di pagamento utilizzato per l'esecuzione di operazioni di pagamento.

"Prestatore di servizi di disposizione di ordine di pagamento" ("PISP"): il prestatore di un servizio che dispone l'ordine di pagamento su richiesta dell'utente di servizi di pagamento relativamente a un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento.

"Prestatore di servizi di pagamento": un organismo di cui all'articolo 1, paragrafo 1, della PSD2[10] o una persona fisica o giuridica che beneficia di un'esenzione ai sensi dell'articolo 32 o 33 della PSD2.

"Utente di servizi di pagamento": persona fisica o giuridica che si avvale di un servizio di pagamento in qualità di pagatore, di beneficiario o di entrambi.

"Dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

"Protezione dei dati fin dalla progettazione": misure tecniche e organizzative, integrate in un prodotto o servizio, volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati.

"Protezione dei dati per impostazione predefinita": adeguate misure tecniche e organizzative, integrate in un prodotto o servizio, che garantiscono che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

"Nome tecniche di regolamentazione": il regolamento delegato (UE) 2018/389 della Commissione, del 27 novembre 2017, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.

"Prestatori terzi": sia i PISP che gli AISP.

1.2 SERVIZI NELL'AMBITO DELLA PSD2

5. La PSD2 introduce due nuovi tipi di (prestatori di) servizi di pagamento: i PISP e gli AISP. Nell'allegato I della PSD2 figurano gli otto servizi di pagamento disciplinati dalla stessa.
6. I "PISP" prestano servizi che dispongono ordini di pagamento su richiesta dell'utente di servizi di pagamento relativamente a un conto di pagamento dell'utente detenuto presso un altro prestatore di servizi di pagamento[11]. Un PISP può richiedere a un ASPSP (generalmente una banca) di disporre un'operazione per conto dell'utente di servizi di pagamento. L'utente (di servizi di pagamento) può essere una persona fisica (interessato) o una persona giuridica.
7. Gli AISP prestano servizi online che forniscono informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento[12]. Secondo quanto affermato al considerando 28 della PSD2, l'utente di servizi di pagamento può disporre imme-

diatamente di un quadro generale della sua situazione finanziaria in un dato momento.

8. Per quanto riguarda i servizi di informazione sui conti, i servizi offerti potrebbero essere di diversi tipi e porre l'accento su caratteristiche e finalità differenti. Alcuni prestatori possono ad esempio offrire agli utenti servizi di pianificazione del bilancio e di monitoraggio della spesa. Il trattamento dei dati personali nell'ambito di tali servizi è disciplinato dalla PSD2. I servizi che comportano valutazioni del merito creditizio dell'utente di servizi di pagamento o i servizi di audit che si basano sulla raccolta di informazioni tramite un servizio di informazione sui conti esulano dall'ambito di applicazione della PSD2 e rientrano pertanto nell'ambito di applicazione del GDPR. Inoltre anche i conti diversi dai conti di pagamento (ad esempio i conti di risparmio e di investimento) non sono contemplati dalla PSD2. In ogni caso, il GDPR è il quadro giuridico applicabile al trattamento dei dati personali.

Esempio 1

HappyPayments è un'impresa che offre un servizio online che consiste nella fornitura di informazioni su uno o più conti di pagamento tramite un'applicazione mobile per consentire il controllo della propria situazione finanziaria (servizio di informazione sui conti). Attraverso tale servizio, l'utente di servizi di pagamento può visualizzare in forma sintetica il saldo e le operazioni recenti relativamente a due o più conti di pagamento detenuti presso banche differenti. Il servizio consente inoltre, a discrezione dell'utente di servizi di pagamento, di classificare le spese e le entrate in funzione di diverse categorie (stipendio, tempo libero, energia, mutuo, ecc.), aiutando così l'utente di servizi di pagamento nella pianificazione finanziaria. Attraverso l'applicazione in questione, HappyPayments offre anche un servizio che dispone pagamenti direttamente dal conto o dai conti di pagamento designati dall'utente (servizio di disposizione di ordine di pagamento).

9. La PSD2 disciplina le condizioni giuridiche alle quali i PISP e gli AISP possono accedere ai conti di pagamento allo scopo di fornire i rispettivi servizi agli utenti di servizi di pagamento.

10. L'articolo 66, paragrafo 1, e l'articolo 67, paragrafo 1, della PSD2 stabiliscono che l'accesso e l'utilizzo dei servizi di pagamento e di informazione sui conti sono diritti dell'utente di servizi di pagamento. Ciò significa che l'utente di servizi di pagamento dovrebbe rimanere totalmente libero per quanto riguarda l'esercizio di tale diritto e non può essere costretto ad avvalersene.

11. L'accesso ai conti di pagamento e l'uso delle informazioni sui conti di pagamento sono in parte disciplinati dagli articoli 66 e 67 della PSD2, che contengono garanzie relative alla protezione dei dati (personali). L'articolo 66, paragrafo 3, lettera f), della PSD2 stabilisce che il PISP non può chiedere all'utente di servizi di pagamento dati diversi da quelli necessari a prestare il

servizio di disposizione di ordine di pagamento, e l'articolo 66, paragrafo 3, lettera g), della PSD2 stabilisce che i PISP non possono usare o conservare dati né accedere ad essi per fini diversi dalla prestazione del servizio di disposizione di ordine di pagamento esplicitamente richiesto dall'utente di servizi di pagamento. L'articolo 67, paragrafo 2, lettera d), della PSD2 limita inoltre l'accesso degli AISP alle informazioni sui conti di pagamento designati e sulle operazioni di pagamento a questi associate, mentre l'articolo 67, paragrafo 2, lettera f), della PSD2 stabilisce che gli AISP non possono usare o conservare dati né accedere ad essi per fini diversi da quelli della prestazione del servizio di informazione sui conti esplicitamente richiesto dall'utente di servizi di pagamento, conformemente alle norme sulla protezione dei dati. L'articolo sottolinea che, nell'ambito dei servizi di informazione sui conti, i dati personali possono essere raccolti solo per finalità determinate, esplicite e legittime. Un AISP dovrebbe pertanto indicare esplicitamente nel contratto per quali finalità specifiche saranno trattati i dati personali relativi alle informazioni sui conti nell'ambito del servizio di informazione sui conti prestato. Il contratto dovrebbe essere lecito, corretto e trasparente ai sensi dell'articolo 5 del GDPR e dovrebbe rispettare anche le altre normative in materia di protezione dei consumatori.

12. A seconda delle circostanze specifiche, i prestatori di servizi di pagamento potrebbero essere titolari del trattamento o responsabili del trattamento ai sensi del GDPR. Ai fini delle presenti linee guida, sono "titolari del trattamento" i prestatori di servizi di pagamento che, singolarmente o insieme ad altri, determinano le finalità e i mezzi del trattamento di dati personali. Ulteriori orientamenti al riguardo sono consultabili nelle linee guida 7/2020 dell'EDPB sulle nozioni di titolare del trattamento e responsabile del trattamento nel GDPR.

2. FONDAMENTI DI LICEITA' E ULTERIORE TRATTAMENTO A NORMA DELLA PSD2

2.1 FONDAMENTI DI LICEITÀ DEL TRATTAMENTO

13. A norma del GDPR, i titolari del trattamento devono disporre di una base giuridica per trattare i dati personali. All'articolo 6, paragrafo 1, del GDPR figura un elenco esaustivo e restrittivo di sei basi giuridiche per il trattamento dei dati personali a norma del regolamento[13]. Spetta al titolare del trattamento definire la base giuridica adatta e garantire che siano soddisfatte tutte le condizioni per l'applicazione di tale base giuridica. La determinazione della base adatta e più appropriata in una specifica situazione dipende dalle circostanze in cui avviene il trattamento, comprese la finalità del trattamento e la relazione intercorrente tra il titolare del trattamento e l'interessato.

2.2 ARTICOLO 6, PARAGRAFO 1, LETTERA B), DEL GDPR (IL TRATTAMENTO È NECESSARIO ALL'ESECUZIONE DI UN CONTRATTO)

14. I servizi di pagamento sono prestati sulla base di un contratto tra l'utente di servizi di pagamento e il prestatore di servizi di pagamento. Come affermato al considerando 87 della PSD2, *"[l]a presente direttiva dovrebbe riguardare solo gli obblighi e le responsabilità contrattuali tra l'utente dei servizi di pagamento e il corrispondente prestatore di servizi di pagamento"*. Nell'ambito del GDPR, la principale base giuridica per il trattamento dei dati personali per la prestazione di servizi di pagamento è l'articolo 6, paragrafo 1, lettera b), per cui il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

15. I servizi di pagamento disciplinati dalla PSD2 sono definiti all'allegato I della stessa. La prestazione di tali servizi, quale definita dalla PSD2, è un requisito per la conclusione di un contratto in cui le parti hanno accesso ai dati relativi al conto di pagamento dell'utente di servizi di pagamento. I prestatori di servizi di pagamento in questione devono inoltre essere operatori autorizzati. Per quanto riguarda i servizi di disposizione di ordine di pagamento e i servizi di informazione sui conti ai sensi della PSD2, i contratti possono includere clausole che stabiliscono anche condizioni relative a servizi aggiuntivi non disciplinati dalla PSD2. Le *linee guida 2/2019 dell'EDPB sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati* chiariscono che i titolari del trattamento devono valutare quale trattamento di dati personali sia oggettivamente necessario per eseguire il contratto. Tali linee guida sottolineano che la giustificazione della necessità dipende dalla natura del servizio, dalle prospettive e dalle aspettative reciproche delle parti contraenti, dalla ratio del contratto e dai suoi elementi essenziali.

16. Le linee guida 2/2019 dell'EDPB chiariscono inoltre che, alla luce dell'articolo 7, paragrafo 4, del GDPR, viene operata una distinzione tra le attività di trattamento necessarie all'esecuzione di un contratto e le clausole che subordinano l'erogazione del servizio a talune attività di trattamento che di fatto non sono necessarie ai fini dell'esecuzione del contratto. Il concetto di "necessario all'esecuzione" richiede chiaramente qualcosa di più di una clausola contrattuale[14]. Il titolare del trattamento dovrebbe essere in grado di dimostrare in che modo l'oggetto principale del contratto specifico stipulato con l'interessato non sia di fatto realizzabile senza lo specifico trattamento dei dati personali in questione. Un mero riferimento al trattamento dei dati o la semplice menzione di tale trattamento in un contratto non è sufficiente a far rientrare il trattamento in questione nell'ambito di applicazione dell'articolo 6, paragrafo 1, lettera b), del GDPR.

17. L'articolo 5, paragrafo 1, lettera b), del GDPR stabilisce il principio della limitazione delle finalità, che impone che i dati personali siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità. Nel valutare se l'articolo 6, paragrafo 1, lettera b), costituisca una base giuridica appropriata per un servizio

(di pagamento) online, si dovrebbe tenere conto dello scopo, della finalità o dell'obiettivo specifico/a del servizio[15]. Le finalità del trattamento devono essere chiaramente specificate e comunicate all'interessato, nel rispetto degli obblighi di limitazione delle finalità e di trasparenza cui il titolare del trattamento è soggetto. La valutazione di ciò che è "necessario" comporta una valutazione combinata, basata sui fatti, del trattamento "per l'obiettivo perseguito e della possibilità che tale trattamento sia meno intrusivo rispetto ad altre opzioni disponibili per il conseguimento del medesimo obiettivo". L'articolo 6, paragrafo 1, lettera b), non si applicherà al trattamento che è utile, ma non oggettivamente necessario per eseguire il servizio oggetto del contratto o per adottare le pertinenti misure precontrattuali su richiesta dell'interessato, anche laddove ciò sia necessario per altre finalità commerciali del titolare del trattamento[16].

18. Le linee guida 2/2019 dell'EDPB chiariscono che un contratto non può ampliare artificiosamente le categorie di dati personali o le tipologie di trattamenti che il titolare necessita di effettuare per l'esecuzione del contratto ai sensi dell'articolo 6, paragrafo 1, lettera b)[17]. In tali linee guida vengono trattati anche i casi in cui si possono creare situazioni del tipo "prendere o lasciare" per gli interessati che intendono usufruire soltanto di uno dei servizi. Ciò può verificarsi quando un titolare del trattamento desidera raggruppare più servizi distinti o elementi di un servizio con finalità, caratteristiche o ratio differenti in un unico contratto. Se il contratto è costituito da più servizi o elementi distinti che di fatto possono ragionevolmente essere prestati indipendentemente l'uno dall'altro, l'applicabilità dell'articolo 6, paragrafo 1, lettera b), dovrebbe essere valutata separatamente nel contesto di ciascuno di tali servizi, considerando ciò che è oggettivamente necessario per ciascuno dei singoli servizi che l'interessato ha attivamente richiesto o sottoscritto[18].

19. Conformemente alle suddette linee guida, i titolari del trattamento devono valutare ciò che è oggettivamente necessario all'esecuzione del contratto. Se i titolari del trattamento non sono in grado dimostrare che il trattamento dei dati personali relativi al conto di pagamento è oggettivamente necessario per la prestazione di ciascun distinto servizio, l'articolo 6, paragrafo 1, lettera b), del GDPR non costituisce una valida base giuridica per il trattamento. In tali casi, il titolare del trattamento dovrebbe valutare la possibilità di fondare il trattamento su un'altra base giuridica.

2.3 PREVENZIONE DELLE FRODI

20. A norma dell'articolo 94, paragrafo 1, della PSD2, gli Stati membri devono autorizzare il trattamento dei dati personali da parte di sistemi di pagamento e di prestatori di servizi di pagamento se necessario per garantire la prevenzione, l'indagine e l'individuazione dei casi di frode nei pagamenti. Il trattamento dei dati personali strettamente necessario per prevenire le frodi potrebbe costituire un interesse legittimo del prestatore di servizi di pagamento in questione, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato[19]. Le attività di trattamento ai fini

della prevenzione delle frodi dovrebbero basarsi su un'attenta valutazione caso per caso da parte del titolare del trattamento, conformemente al principio di responsabilizzazione. Inoltre i titolari del trattamento possono anche essere soggetti a specifici obblighi giuridici che richiedono il trattamento di dati personali allo scopo di prevenire le frodi.

2.4 ULTERIORE TRATTAMENTO (AISP E PISP)

21. L'articolo 6, paragrafo 4, del GDPR stabilisce le condizioni affinché i dati personali possano essere trattati per una finalità diversa da quella per la quale sono stati raccolti. Più nello specifico, tale ulteriore trattamento può avere luogo se si basa su un atto legislativo dell'Unione o degli Stati membri che costituisce una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, se l'interessato ha prestato il proprio consenso o se il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti è compatibile con la finalità iniziale.
22. Occorre considerare con attenzione l'articolo 66, paragrafo 3, lettera g), e l'articolo 67, paragrafo 2, lettera f), della PSD2. Come sottolineato in precedenza, l'articolo 66, paragrafo 3, lettera g), della PSD2 stabilisce che il PISP non può usare o conservare dati né accedere ad essi per fini diversi dalla prestazione del servizio di disposizione di ordine di pagamento esplicitamente richiesto dal pagatore. L'articolo 67, paragrafo 2, lettera f), della PSD2 stabilisce che l'AISP non può usare o conservare dati né accedere a essi per fini diversi da quelli della prestazione del servizio di informazione sui conti esplicitamente richiesto dall'utente di servizi di pagamento, conformemente alle norme sulla protezione dei dati.
23. Di conseguenza l'articolo 66, paragrafo 3, lettera g), e l'articolo 67, paragrafo 2, lettera f), della PSD2 limitano considerevolmente le possibilità di trattamento per altre finalità, il che significa che il trattamento per un'altra finalità non è consentito, a meno che l'interessato abbia prestato il proprio consenso a norma dell'articolo 6, paragrafo 1, lettera a), del GDPR o che il trattamento sia previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, a norma dell'articolo 6, paragrafo 4, del GDPR. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri, le limitazioni di cui all'articolo 66, paragrafo 3, lettera g), e all'articolo 67, paragrafo 2, lettera f), della PSD2 chiariscono che qualsiasi altra finalità non è compatibile con la finalità per la quale i dati personali sono inizialmente raccolti. Il test di compatibilità di cui all'articolo 6, paragrafo 4, del GDPR non può dar luogo a una base giuridica per il trattamento.
24. L'articolo 6, paragrafo 4, del GDPR consente un ulteriore trattamento sulla base del diritto dell'Unione o degli Stati membri. Ad esempio, tutti i PISP e gli AISP sono soggetti obbligati ai sensi dell'articolo 3, punto 2), lettera a),

della direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo. Tali soggetti obbligati sono pertanto tenuti ad applicare le misure di adeguata verifica della clientela specificate nella direttiva. I dati personali trattati nell'ambito di un servizio disciplinato dalla PSD2 sono dunque soggetti a un ulteriore trattamento sulla base di almeno un obbligo giuridico gravante sul prestatore di servizi[20].

25. Come indicato al punto 20, l'articolo 6, paragrafo 4, del GDPR prevede che il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti possa basarsi sul consenso dell'interessato, qualora siano soddisfatte tutte le condizioni per la prestazione del consenso stabilite dal regolamento. Come sottolineato in precedenza, il titolare del trattamento deve dimostrare che sussiste la possibilità di rifiutare o revocare il consenso senza subire un pregiudizio (considerando 42 del GDPR).

2.5 MOTIVO LECITO PER CONCEDERE L'ACCESSO AL CONTO (ASPSP)

26. Come sottolineato al punto 10, gli utenti di servizi di pagamento possono esercitare il diritto di avvalersi di servizi di disposizione di ordine di pagamento e di informazione sui conti. Gli obblighi gravanti sugli Stati membri a norma dell'articolo 66, paragrafo 1, e dell'articolo 67, paragrafo 1, della PSD2 dovrebbero essere recepiti nell'ordinamento nazionale al fine di garantire l'efficace applicazione del diritto dell'utente di servizi di pagamento di beneficiare dei suddetti servizi di pagamento. L'effettiva applicazione di tali diritti non sarebbe possibile senza l'esistenza di un corrispondente obbligo per l'ASPSP, generalmente una banca, di concedere l'accesso al conto al prestatore di servizi di pagamento, a condizione che quest'ultimo soddisfi tutti i requisiti per ottenere l'accesso al conto dell'utente di servizi di pagamento. Inoltre l'articolo 66, paragrafo 5, e l'articolo 67, paragrafo 4, della PSD2 stabiliscono chiaramente che la prestazione di servizi di disposizione di ordine di pagamento e di servizi di informazione sui conti non è subordinata all'esistenza di un rapporto contrattuale tra il PISP/AISP e l'ASPSP.

27. Il trattamento di dati personali da parte dell'ASPSP che consiste nel concedere l'accesso ai dati personali richiesti dal PISP e dall'AISP affinché essi possano prestare i propri servizi di pagamento all'utente di servizi di pagamento si basa su un obbligo giuridico. Per conseguire gli obiettivi della PSD2, gli ASPSP devono fornire i dati personali ai PISP e agli AISP, condizione necessaria affinché questi ultimi possano prestare i propri servizi, garantendo in tal modo l'applicazione dei diritti di cui all'articolo 66, paragrafo 1, e all'articolo 67, paragrafo 1, della PSD2. La base giuridica applicabile nel caso di specie è dunque l'articolo 6, paragrafo 1, lettera c), del GDPR.

28. Poiché il GDPR specifica che il trattamento basato su un obbligo giuridico dovrebbe essere chiaramente stabilito dal diritto dell'Unione o degli Stati membri (cfr. l'articolo 6, paragrafo 3, del GDPR), l'obbligo per gli ASPSP di concedere l'accesso dovrebbe essere sancito dall'ordinamento nazionale che recepisce la PSD2.

3. CONSENSO ESPLICITO

3.1 CONSENSO AI SENSI DEL GDPR

29. A norma del GDPR, il consenso è una delle sei basi giuridiche che determinano la liceità del trattamento dei dati personali. L'articolo 4, punto 11), del GDPR definisce il consenso come "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento". Queste quattro condizioni – libero, specifico, informato e inequivocabile – sono essenziali affinché il consenso sia valido. Secondo le linee guida 5/2020 dell'EDPB sul consenso ai sensi del regolamento (UE) 2016/679, il consenso può costituire la base legittima appropriata solo se all'interessato vengono offerti il controllo e l'effettiva possibilità di scegliere se accettare i termini proposti o rifiutarli senza subire pregiudizio. Quando richiede il consenso, il titolare del trattamento deve valutare se questo soddisferà tutti i requisiti per essere valido. Se ottenuto nel pieno rispetto del GDPR, il consenso è uno strumento che fornisce all'interessato il controllo sul trattamento dei dati personali che lo riguardano. In caso contrario, il controllo diventa illusorio e il consenso non costituirà una base giuridica valida per il trattamento, rendendo illecita l'attività di trattamento[21].

30. Il GDPR contiene inoltre ulteriori garanzie all'articolo 7, il quale stabilisce che il titolare del trattamento deve essere in grado di dimostrare l'esistenza di un consenso valido al momento del trattamento. La richiesta di consenso deve altresì essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. L'interessato deve inoltre essere informato del diritto di revocare il consenso in qualsiasi momento, con la stessa facilità con cui lo ha accordato.

31. A norma dell'articolo 9 del GDPR, il consenso costituisce una delle eccezioni al divieto generale di trattamento di categorie particolari di dati personali. In tal caso il consenso dell'interessato deve tuttavia essere "esplicito"[22].

32. Secondo le linee guida 5/2020 dell'EDPB sul consenso ai sensi del regolamento (UE) 2016/679, il termine "consenso esplicito" ai sensi del GDPR si riferisce al modo in cui il consenso è espresso dall'interessato e significa che l'interessato deve fornire una dichiarazione esplicita di consenso per finalità di trattamento specifiche. Un modo ovvio per assicurarsi che il consenso sia esplicito consisterebbe nel confermare espressamente il consenso in una dichiarazione scritta. Se del caso, il titolare del trattamento potrebbe assicurarsi che la dichiarazione scritta sia firmata dall'interessato, al fine di dissipare tutti i possibili dubbi e la potenziale mancanza di prove in futuro.

33. In nessun caso il consenso può essere dedotto da dichiarazioni o azioni potenzialmente ambigue. Il titolare del trattamento deve inoltre fare attenzione al fatto che il consenso non può essere ottenuto tramite la stessa azione con cui si accetta un contratto o le condizioni generali di servizio.

3.2 CONSENSO AI SENSI DELLA PSD2

34. L'EDPB rileva che il quadro giuridico relativo al consenso esplicito è complesso, poiché la nozione di "consenso esplicito" figura sia nella PSD2 che nel GDPR. Ciò porta a chiedersi se il "consenso esplicito" di cui all'articolo 94, paragrafo 2, della PSD2 debba essere interpretato allo stesso modo del consenso esplicito ai sensi del GDPR.

3.2.1 CONSENSO ESPLICITO AI SENSI DELL'ARTICOLO 94, PARAGRAFO 2, DELLA PSD2

35. La PSD2 contiene una serie di norme specifiche relative al trattamento dei dati personali, in particolare all'articolo 94, paragrafo 1, che stabilisce che il trattamento dei dati personali ai fini della PSD2 deve essere conforme al diritto dell'UE in materia di protezione dei dati. L'articolo 94, paragrafo 2, della PSD2 stabilisce inoltre che i prestatori di servizi di pagamento possono avere accesso, trattare e conservare i dati personali necessari alla prestazione dei rispettivi servizi di pagamento solo dietro consenso esplicito dell'utente di servizi di pagamento. A norma dell'articolo 33, paragrafo 2, della PSD2, il requisito del consenso esplicito dell'utente di servizi di pagamento non si applica agli AISP. Tuttavia l'articolo 67, paragrafo 2, lettera a), della PSD2 prevede ancora il consenso esplicito affinché gli AISP possano prestare il proprio servizio.

36. Come sottolineato in precedenza, l'elenco delle basi giuridiche per il trattamento a norma del GDPR è esaustivo. Come indicato al punto 14, la base giuridica per il trattamento dei dati personali per la prestazione di servizi di pagamento è, in linea di principio, l'articolo 6, paragrafo 1, lettera b), del GDPR, per cui il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso. Ne consegue che l'articolo 94, paragrafo 2, della PSD2 non può essere considerato una base giuridica supplementare per il trattamento dei dati personali. L'EDPB ritiene che, alla luce di quanto precede, tale paragrafo debba essere interpretato, da un lato, in maniera coerente con il quadro giuridico applicabile in materia di protezione dei dati e, dall'altro, in modo da preservarne l'effetto utile. Il consenso esplicito ai sensi dell'articolo 94, paragrafo 2, della PSD2 dovrebbe pertanto essere considerato un requisito aggiuntivo di natura contrattuale[23] in relazione all'accesso ai dati personali, al loro successivo trattamento e alla loro successiva conservazione ai fini della prestazione di servizi di pagamento e non equivale pertanto al consenso (esplicito) ai sensi del GDPR.

37. Il "consenso esplicito" di cui all'articolo 94, paragrafo 2, della PSD2 è un consenso contrattuale. Ciò implica che l'articolo 94, paragrafo 2, della PSD2 dovrebbe essere interpretato nel senso che, al momento di stipulare un contratto con un prestatore di servizi di pagamento ai sensi della PSD2, gli interessati devono essere pienamente informati delle categorie specifiche di dati personali che saranno trattati. Inoltre devono essere informati della finalità specifica (servizio di pagamento) per la quale i loro dati personali

saranno trattati e devono accettare esplicitamente tali clausole. Queste ultime dovrebbero essere chiaramente distinguibili dalle altre materie che sono oggetto del contratto e dovrebbero essere accettate in maniera esplicita dall'interessato.

38. Fondamentale per la nozione di "consenso esplicito" di cui all'articolo 94, paragrafo 2, della PSD2 è l'ottenimento dell'accesso ai dati personali per il loro successivo trattamento e la loro successiva conservazione ai fini della prestazione di servizi di pagamento[24]. Ciò implica che il prestatore di servizi di pagamento non sta ancora trattando i dati personali, ma deve avere accesso a dati personali trattati sotto la responsabilità di un altro titolare del trattamento. Se un utente di servizi di pagamento stipula ad esempio un contratto con un prestatore di servizi di disposizione di ordine di pagamento, tale prestatore deve ottenere l'accesso ai dati personali dell'utente di servizi di pagamento trattati sotto la responsabilità del prestatore di servizi di pagamento di radicamento del conto. L'oggetto del consenso esplicito di cui all'articolo 94, paragrafo 2, della PSD2 è il permesso di accedere a tali dati personali e di trattarli e conservarli in quanto necessari ai fini della prestazione del servizio di pagamento. Se l'interessato fornisce il consenso esplicito, il prestatore di servizi di pagamento di radicamento del conto è tenuto a concedere l'accesso ai dati personali indicati.

39. Sebbene il consenso di cui all'articolo 94, paragrafo 2, della PSD2 non costituisca una base giuridica per il trattamento dei dati personali, tale consenso è specificamente correlato ai dati personali e alla protezione dei dati e garantisce trasparenza e un certo grado di controllo all'utente di servizi di pagamento[25]. Benché la PSD2 non specifichi le condizioni sostanziali per il consenso ai sensi dell'articolo 94, paragrafo 2, della PSD2, essa dovrebbe essere interpretata, come indicato in precedenza, in maniera coerente con il quadro giuridico applicabile in materia di protezione dei dati e in modo da preservarne l'effetto utile.

40. Per quanto riguarda le informazioni che devono essere fornite dai titolari del trattamento e il requisito di trasparenza, le linee guida del gruppo di lavoro Articolo 29 sulla trasparenza specificano che "*[u]na considerazione centrale al principio della trasparenza evidenziata in queste disposizioni è che l'interessato dovrebbe essere in grado di determinare in anticipo quali siano la portata del trattamento e le relative conseguenze e non dovrebbe successivamente essere colto di sorpresa dalle modalità di utilizzo dei dati personali che lo riguardano*"[26].

41. Inoltre, come richiesto dal principio della limitazione delle finalità, i dati personali devono essere raccolti per finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b), del GDPR). Se i dati personali sono raccolti per più di una finalità, i titolari del trattamento dovrebbero evitare di indicare un'unica finalità generica per giustificare varie ulteriori attività di trattamento che in realtà sono solo lontanamente collegate all'effettiva finalità iniziale[27]. L'EDPB ha evidenziato, da ultimo in riferimento ai contratti riguardanti servizi online, il rischio di inclusione di condizioni generali di trattamento nei contratti e ha affermato che la finalità della raccolta dai dati dovrebbe essere indicata in maniera chiara e specifica: tale finalità dovrebbe

essere sufficientemente dettagliata da consentire di stabilire quale tipo di trattamento è incluso nella finalità specifica e quale no, nonché da consentire di valutare il rispetto della legge e l'applicazione delle garanzie in materia di protezione dei dati[28].

42. Se esaminato alla luce del requisito aggiuntivo del consenso esplicito ai sensi dell'articolo 94, paragrafo 2, della PSD2, ciò implica che i titolari del trattamento devono fornire agli interessati informazioni specifiche ed esplicite sulle finalità specifiche indicate dal titolare del trattamento per la richiesta di accesso, trattamento e conservazione dei loro dati. In linea con l'articolo 94, paragrafo 2, della PSD2, gli interessati devono accettare esplicitamente tali finalità specifiche.

43. Inoltre, come indicato al punto 10, l'EDPB sottolinea che l'utente di servizi di pagamento deve poter scegliere se utilizzare o meno il servizio e non può essere costretto ad avvalersene. Pertanto anche il consenso ai sensi dell'articolo 94, paragrafo 2, della PSD2 deve essere prestato liberamente.

3.3 CONCLUSIONI

44. Il consenso esplicito ai sensi della PSD2 è diverso dal consenso (esplicito) ai sensi del GDPR. Il consenso esplicito ai sensi dell'articolo 94, paragrafo 2, della PSD2 è un requisito aggiuntivo di natura contrattuale. Quando un prestatore di servizi di pagamento necessita di accedere ai dati personali per la prestazione di un servizio di pagamento, è necessario il consenso esplicito dell'utente di servizi di pagamento ai sensi dell'articolo 94, paragrafo 2, della PSD2.

4. TRATTAMENTO DEI DATI DEI TACITI INTERESSATI

4.1 DATI DEI TACITI INTERESSATI

45. Una questione riguardante la protezione dei dati che richiede un esame attento è il trattamento dei cosiddetti "dati dei taciti interessati" (*silent party data*). Nell'ambito del presente documento, i dati dei taciti interessati sono dati personali di interessati che non sono utenti di uno specifico prestatore di servizi di pagamento, ma i cui dati personali sono trattati da tale specifico prestatore di servizi di pagamento ai fini dell'esecuzione di un contratto tra il prestatore e un utente di servizi di pagamento. Ciò si verifica ad esempio nel caso in cui un utente di servizi di pagamento, l'interessato A, si avvale dei servizi di un AISP, e l'interessato B ha effettuato una serie di operazioni di pagamento sul conto di pagamento dell'interessato A. In questo caso, l'interessato B è considerato "tacito interessato" e i suoi dati personali (come il suo numero di conto e l'importo oggetto di tali operazioni) sono considerati "dati del tacito interessato".

4.2 INTERESSE LEGITTIMO DEL TITOLARE DEL TRATTAMENTO

46. L'articolo 5, paragrafo 1, lettera b), del GDPR stabilisce che i dati personali devono essere raccolti solamente per finalità determinate, esplicite e legittime e non possono essere successivamente trattati in modo che sia incompatibile con tali finalità. Inoltre il GDPR prevede che qualsiasi trattamento di dati personali debba essere necessario, proporzionato e in linea con i principi di protezione dei dati, quali la limitazione delle finalità e la minimizzazione dei dati.
47. Il GDPR può consentire il trattamento dei dati dei taciti interessati qualora sia necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi (articolo 6, paragrafo 1, lettera f), del GDPR). Tale trattamento può tuttavia avere luogo solo a condizione che "gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali" non prevalgano rispetto al legittimo interesse del titolare del trattamento.
48. Una base lecita per il trattamento dei dati dei taciti interessati da parte dei PISP e degli AISP – nell'ambito della prestazione di servizi di pagamento di cui alla PSD2 – potrebbe quindi essere il legittimo interesse del titolare del trattamento o di terzi a dare esecuzione al contratto stipulato con l'utente di servizi di pagamento. La necessità di trattare i dati personali dei taciti interessati è limitata e determinata dalle ragionevoli aspettative di tali interessati. Nell'ambito della prestazione dei servizi di pagamento disciplinati dalla PSD2 devono essere adottate misure efficaci e adeguate a garantire che non vengano lesi gli interessi o i diritti e le libertà fondamentali dei taciti interessati e che siano rispettate le ragionevoli aspettative di tali interessati riguardo al trattamento dei loro dati personali. A tale riguardo, il titolare del trattamento (AISP o PISP) deve predisporre le garanzie riguardanti il trattamento necessarie a tutelare i diritti degli interessati. Ciò comprende misure tecniche volte ad assicurare che i dati dei taciti interessati non siano trattati per una finalità diversa da quella per la quale i dati personali sono stati inizialmente raccolti dai PISP e dagli AISP. Se possibile, dovrebbero essere utilizzate anche tecniche di cifratura o altre modalità che consentano di raggiungere un livello adeguato di sicurezza e di minimizzazione dei dati.

4.3 ULTERIORE TRATTAMENTO DEI DATI PERSONALI DEI TACITI INTERESSATI

49. Come sottolineato al punto 29, i dati personali trattati in relazione a un servizio di pagamento disciplinato dalla PSD2 potrebbero essere ulteriormente trattati in funzione di obblighi giuridici gravanti sul prestatore di servizi. Tali obblighi giuridici potrebbero riguardare i dati personali dei taciti interessati.
50. Per quanto riguarda l'ulteriore trattamento dei dati dei taciti interessati sulla base di un legittimo interesse, l'EDPB è del parere che tali dati non possano essere utilizzati per una finalità diversa da quella per la quale i dati personali sono stati raccolti, a meno che ciò non sia previsto dal diritto dell'UE o

degli Stati membri. Ottenere il consenso dei taciti interessati non è giuridicamente possibile, poiché per farlo sarebbe necessario raccogliere o trattare i dati personali dei taciti interessati, operazioni per le quali non è possibile ravvisare alcuna base giuridica a norma dell'articolo 6 del GDPR. Nemmeno il criterio di compatibilità di cui all'articolo 6, paragrafo 4, del GDPR può fornire una base per il trattamento dei dati per altre finalità (ad esempio attività di marketing diretto). I diritti e le libertà dei taciti interessati[29] non vengono rispettati se il nuovo titolare del trattamento utilizza i dati personali per altre finalità, tenendo conto del contesto in cui tali dati sono stati raccolti, in particolare dell'assenza di qualsiasi relazione con i taciti interessati, dell'assenza di qualsiasi legame tra ogni altra finalità e la finalità per la quale i dati personali sono stati inizialmente raccolti (ossia il fatto che i prestatori di servizi di pagamento necessitano dei dati dei taciti interessati soltanto per dare esecuzione a un contratto con l'altra parte contraente), della natura dei dati personali in questione[30] e del fatto che gli interessati non possono ragionevolmente aspettarsi un ulteriore trattamento né tantomeno sapere quale titolare del trattamento possa trattare i loro dati personali, e date le restrizioni giuridiche al trattamento di cui all'articolo 66, paragrafo 3, lettera g), e all'articolo 67, paragrafo 2, lettera f), della PSD2.

5. TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI A NORMA DELLA PSD2

5.1 CATEGORIE PARTICOLARI DI DATI PERSONALI

51. A norma dell'articolo 9, paragrafo 1, del GDPR, "[è] vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".

52. È opportuno sottolineare che in alcuni Stati membri i pagamenti elettronici sono già ampiamente diffusi e molte persone li preferiscono al contante nelle operazioni quotidiane. Al tempo stesso, le operazioni finanziarie possono rivelare informazioni sensibili su un singolo interessato, comprese quelle relative a categorie particolari di dati personali. Ad esempio, a seconda dei dettagli dell'operazione, eventuali donazioni a partiti o organizzazioni politiche, chiese o parrocchie possono rivelare opinioni politiche e convinzioni religiose. L'affiliazione a un sindacato può essere rivelata dall'addebito di una quota associativa annuale sul conto bancario di una persona. Analizzando le parcelle mediche pagate da un interessato a un professionista del settore medico (ad esempio uno psichiatra) è possibile raccogliere dati personali relativi alla salute. Infine le informazioni su taluni acquisti possono rivelare informazioni relative alla vita sessuale o all'orientamento sessuale di una persona. Come dimostrato da questi esempi, anche singole operazioni possono contenere categorie particolari di dati personali. Inoltre i servizi di in-

formazione sui conti potrebbero avvalersi della profilazione quale definita all'articolo 4, punto 4), del GDPR. Come già sottolineato dalle linee guida del gruppo di lavoro Articolo 29 sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, approvate dall'EDPB, "la profilazione può creare dati appartenenti a categorie particolari desumendoli da dati che di per sé non appartengono a categorie particolari ma che diventano tali se combinati con altri dati."[31] Ciò significa che da un insieme di operazioni finanziarie possono emergere diversi tipi di modelli comportamentali, che possono includere categorie particolari di dati personali. È pertanto molto probabile che un prestatore di servizi che tratta informazioni relative alle operazioni finanziarie degli interessati tratti anche categorie particolari di dati personali.

53. Per quanto riguarda il termine "dati sensibili relativi ai pagamenti", l'EDPB osserva quanto segue. La definizione dei dati sensibili relativi ai pagamenti contenuta nella PSD2 diverge notevolmente dall'accezione del termine "dati personali sensibili" come comunemente utilizzata nell'ambito del GDPR e della (normativa sulla) protezione dei dati. Mentre la PSD2 definisce i dati sensibili relativi ai pagamenti come "dati che possono essere usati per commettere frodi, incluse le credenziali di sicurezza personalizzate", il GDPR sottolinea la necessità di prevedere una specifica protezione per categorie particolari di dati personali che, a norma dell'articolo 9, sono per loro natura particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, come le categorie particolari di dati personali[32]. A tale riguardo si raccomanda almeno di mappare e classificare con precisione il tipo di dati personali che saranno trattati. Molto probabilmente sarà necessaria una valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 del GDPR, che contribuirà a tale esercizio di mappatura. Ulteriori orientamenti sulle valutazioni d'impatto sulla protezione dei dati sono consultabili nelle linee guida del gruppo di lavoro Articolo 29 in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, approvate dall'EDPB.

5.2 DEROGHE POSSIBILI

54. Il divieto di cui all'articolo 9 del GDPR non è assoluto. In particolare, mentre le deroghe di cui all'articolo 9, paragrafo 2, lettere da b) a f) e da h) a j), del GDPR non sono evidentemente applicabili al trattamento dei dati personali nell'ambito della PSD2, si potrebbero prendere in considerazione le due seguenti deroghe di cui all'articolo 9, paragrafo 2, del GDPR:

a) il divieto non si applica se l'interessato ha prestato il proprio consenso esplicito al trattamento dei dati personali in questione per una o più finalità specifiche (articolo 9, paragrafo 2, lettera a), del GDPR);

b) il divieto non si applica se il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del

diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (articolo 9, paragrafo 2, lettera g), del GDPR).

55. È opportuno sottolineare che l'elenco delle deroghe di cui all'articolo 9, paragrafo 2, del GDPR è esaustivo. La possibilità che categorie particolari di dati personali siano incluse nei dati personali trattati per la prestazione di uno qualsiasi dei servizi che rientrano nell'ambito di applicazione della PSD2 deve essere riconosciuta dal prestatore di servizi. Poiché il divieto di cui all'articolo 9, paragrafo 1, del GDPR è applicabile a tali prestatori di servizi, questi ultimi devono garantire che una delle deroghe di cui all'articolo 9, paragrafo 2, del GDPR sia applicabile alla loro situazione. È opportuno sottolineare che, qualora il prestatore di servizi non sia in grado di dimostrare l'applicazione di una delle deroghe, vige il divieto di cui all'articolo 9, paragrafo 1.

5.3 INTERESSE PUBBLICO RILEVANTE

56. I servizi di pagamento possono trattare categorie particolari di dati personali per motivi di interesse pubblico rilevante, ma solo quando sono soddisfatte tutte le condizioni di cui all'articolo 9, paragrafo 2, lettera g), del GDPR. Ciò significa che il trattamento delle categorie particolari di dati personali deve essere l'oggetto di una specifica deroga all'articolo 9, paragrafo 1, del GDPR sancita dal diritto dell'Unione o degli Stati membri. Tale disposizione dovrà essere proporzionata alla finalità perseguita dal trattamento e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. La disposizione sancita dal diritto dell'Unione o degli Stati membri dovrà inoltre rispettare l'essenza del diritto alla protezione dei dati. Infine occorre dimostrare anche che il trattamento delle categorie particolari di dati è necessario per motivi di interesse pubblico rilevante, compresi interessi di importanza sistemica. Solo laddove tutte le suddette condizioni siano pienamente soddisfatte, la deroga potrebbe essere applicata a determinati tipi di servizi di pagamento.

5.4 CONSENSO ESPLICITO

57. Nei casi in cui non trova applicazione la deroga di cui all'articolo 9, paragrafo 2, lettera g), del GDPR, ottenere il consenso esplicito dell'interessato nel rispetto delle condizioni stabilite nel GDPR affinché il consenso sia valido sembra rimanere l'unica possibile deroga lecita per il trattamento delle categorie particolari di dati personali da parte di prestatori terzi. Le linee guida 5/2020 dell'EDPD sul consenso ai sensi del regolamento (UE) 2016/679 affermano[33] che "[l]'articolo 9, paragrafo 2, non riconosce il trattamento "necessario all'esecuzione di un contratto" come un'eccezione al divieto generale di trattare categorie particolari di dati. Di conseguenza i titolari del trattamento e gli Stati membri che rientrano nel contesto di applicazione di tale circostanza

dovrebbero esaminare le eccezioni specifiche di cui all'articolo 9, paragrafo 2, lettere da b) a j)". Quando i prestatori di servizi si basano sull'articolo 9, paragrafo 2, lettera a), del GDPR, devono assicurarsi che sia stato loro accordato il consenso esplicito prima di iniziare il trattamento. Il consenso esplicito di cui all'articolo 9, paragrafo 2, lettera a), del GDPR deve soddisfare tutti i requisiti stabiliti dal regolamento.

5.5 ASSENZA DI DEROGHE APPLICABILI

58. Come sottolineato in precedenza, qualora il prestatore di servizi non sia in grado di dimostrare l'applicabilità di una delle deroghe, vige il divieto di cui all'articolo 9, paragrafo 1. In questo caso si potrebbero adottare misure tecniche volte a impedire il trattamento di categorie particolari di dati personali, ad esempio impedendo il trattamento di alcuni punti dati. A tale riguardo, i prestatori di servizi di pagamento possono esaminare le opzioni tecniche disponibili per escludere categorie particolari di dati personali e consentire un accesso selezionato che impedisca il trattamento di categorie particolari di dati personali relativi a taciti interessati da parte di prestatori terzi.

6. MINIMIZZAZIONE DEI DATI, SICUREZZA, TRASPARENZA, RESPONSABILIZZAZIONE E PROFILAZIONE

6.1 MINIMIZZAZIONE DEI DATI E PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA

59. Il principio della minimizzazione dei dati è sancito dall'articolo 5, paragrafo 1, lettera c), del GDPR: "I dati personali sono [...] adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati". In base al principio della minimizzazione dei dati, i titolari del trattamento essenzialmente non dovrebbero trattare più dati personali di quanto necessario per conseguire la specifica finalità perseguita. Come indicato nel capitolo 2, la quantità e il tipo di dati personali necessari per prestare il servizio di pagamento sono determinati dall'obiettivo e dall'oggetto essenziale del contratto come inteso da entrambe le parti[34]. La minimizzazione dei dati è applicabile a ogni trattamento (ad esempio a ogni raccolta o richiesta di dati personali o a ogni accesso a dati personali). Le linee guida 4/2019 dell'EDPB sulla protezione dei dati fin dalla progettazione e per impostazione predefinita a norma dell'articolo 25 del GDPR stabiliscono che anche i responsabili del trattamento e i fornitori di tecnologie sono riconosciuti come promotori essenziali della protezione dei dati fin dalla progettazione e per impostazione predefinita; essi dovrebbero inoltre essere consapevoli del fatto che i titolari del trattamento sono tenuti a trattare i dati personali solo con sistemi e tecnologie caratterizzati da una protezione dei dati integrata[35].
60. L'articolo 25 del GDPR sancisce l'obbligo di applicazione della protezione dei dati fin dalla progettazione e per impostazione predefinita. Tale obbligo è

particolarmente importante per il principio della minimizzazione dei dati. A norma del suddetto articolo, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati. Il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. Tali misure possono comprendere la cifratura, la pseudonimizzazione e altre misure tecniche.

61. Quando si applica l'obbligo di cui all'articolo 25 del GDPR, occorre tenere conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche dei rischi di probabilità e gravità variabili per i diritti e le libertà delle persone fisiche comportati dal trattamento. Ulteriori chiarimenti in merito a tale obbligo vengono forniti nelle già menzionate linee guida 4/2019 dell'EDPB sulla protezione dei dati fin dalla progettazione e per impostazione predefinita a norma dell'articolo 25.

6.2 MISURE DI MINIMIZZAZIONE DEI DATI

62. Il prestatore terzo che accede ai dati del conto di pagamento al fine di fornire i servizi richiesti deve tenere conto anche del principio di minimizzazione dei dati e deve raccogliere solo i dati personali necessari per fornire gli specifici servizi di pagamento richiesti dall'utente di servizi di pagamento. In linea di principio, l'accesso ai dati personali dovrebbe essere limitato a quanto necessario per la prestazione dei servizi di pagamento. Come sottolineato nel capitolo 2, a norma della PSD2 gli ASPSP sono tenuti a condividere le informazioni dell'utente di servizi di pagamento su richiesta di quest'ultimo, quando questi intenda utilizzare un servizio di disposizione di ordine di pagamento o un servizio di informazione sui conti.

63. Qualora non tutti i dati relativi al conto di pagamento siano necessari per l'esecuzione del contratto, l'AISP dovrebbe selezionare le categorie di dati pertinenti prima che i dati vengano raccolti. Tra le categorie di dati che potrebbero non essere necessarie possono figurare ad esempio l'identità del tacito interessato e le caratteristiche dell'operazione. Inoltre, a meno che non sia richiesto dal diritto degli Stati membri o dell'Unione, può non essere necessario indicare l'IBAN del conto bancario del tacito interessato.

64. A tale proposito potrebbe essere presa in considerazione, nell'ambito dell'attuazione di politiche adeguate in materia di protezione dei dati, in linea con l'articolo 24, paragrafo 2, del GDPR, l'eventuale applicazione di misure tecniche che consentano o favoriscano l'adempimento dell'obbligo, da par-

te dei prestatori terzi, di accedere e reperire solo i dati personali necessari per la fornitura dei loro servizi. A tale riguardo, l'EDPB raccomanda l'uso di strumenti digitali che aiutino gli AISP a ottemperare all'obbligo di raccogliere solo i dati personali necessari per le finalità per le quali viene effettuato il trattamento. Ad esempio, quando un prestatore di servizi non necessita delle caratteristiche delle operazioni (indicate nel campo delle registrazioni destinato alla descrizione delle operazioni) per la fornitura del suo servizio, uno strumento digitale di selezione potrebbe consentire ai prestatori terzi di escludere il campo in questione dalle attività di trattamento complessive da loro svolte.

Esempio 2

HappyPayments, il prestatore di servizi di informazione sui conti di cui all'esempio 1, vuole assicurarsi di trattare solo i dati personali relativi ai conti di pagamento cui i suoi utenti sono interessati. Chiedere l'accesso a un maggior numero di dati relativi ai conti di pagamento non sarebbe infatti necessario per la prestazione del servizio. HappyPayments consente dunque agli utenti di selezionare le tipologie specifiche di informazioni cui sono interessati.

L'utente A vuole avere una visione d'insieme delle proprie spese negli ultimi due mesi. Pertanto richiede, in relazione ai suoi due conti bancari, detenuti presso due diversi ASPSP, le informazioni riguardanti tutte le operazioni degli ultimi due mesi, l'importo delle operazioni, la data di esecuzione e il nome del destinatario, e seleziona le caselle corrispondenti nell'interfaccia utente di HappyPayments.

HappyPayments inizia dunque a richiedere ai rispettivi ASPSP solo le informazioni corrispondenti ai campi selezionati dall'utente A e solo per il periodo degli ultimi due mesi. Non vengono richieste informazioni quali la "comunicazione" del trasferimento o l'IBAN, in quanto l'utente A non ha richiesto tali informazioni.

Per permettere a HappyPayments di ottemperare ai propri obblighi di minimizzazione dei dati, gli ASPSP consentono a HappyPayments di richiedere campi specifici per una serie di date.

65. A tale proposito è inoltre opportuno osservare che, a norma della PSD2, gli ASPSP sono autorizzati a fornire l'accesso solo alle informazioni sui conti di pagamento. La PSD2 non prevede alcuna base giuridica che consenta l'accesso ai dati personali contenuti in altri conti, quali conti di risparmio, conti ipotecari o conti di investimento. Di conseguenza, a norma della PSD2, devono essere attuate misure tecniche per garantire che l'accesso sia limitato alle informazioni sui conti di pagamento necessarie.

66. Oltre a raccogliere il minor numero possibile di dati, il prestatore di servizi deve anche applicare periodi di conservazione limitati. I dati personali non dovrebbero essere conservati dal prestatore di servizi per un periodo supe-

riore a quello necessario per le finalità indicate dall'utente di servizi di pagamento.

67. Se il contratto tra l'interessato e l'AISP richiede la trasmissione di dati personali a terzi, possono essere trasmessi solo i dati personali necessari per l'esecuzione del contratto. Gli interessati dovrebbero inoltre essere specificamente informati della trasmissione e dei dati personali che saranno trasmessi ai terzi in questione.

6.3 SICUREZZA

68. L'EDPB ha già sottolineato che la violazione dei dati personali finanziari "*implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato*" e cita a titolo di esempio i rischi di frodi relative ai pagamenti[36].

69. Se una violazione dei dati riguarda dati finanziari, l'interessato può essere esposto a rischi considerevoli. A seconda delle informazioni violate, gli interessati possono essere esposti al rischio di furto d'identità e furto dei fondi nei loro conti e di altri beni. Vi è inoltre la possibilità che l'esposizione dei dati sulle operazioni comporti notevoli rischi per la privacy, in quanto i dati relativi alle operazioni possono contenere riferimenti a tutti gli aspetti della vita privata dell'interessato. Allo stesso tempo, i dati finanziari sono ovviamente preziosi per i criminali e rappresentano quindi un bersaglio allettante.

70. In qualità di titolari del trattamento, i prestatori di servizi di pagamento sono tenuti ad adottare misure adeguate per proteggere i dati personali degli interessati (articolo 24, paragrafo 1, del GDPR). Quanto più alti sono i rischi associati all'attività di trattamento svolta dal titolare del trattamento, tanto più rigorose sono le norme di sicurezza che devono essere applicate. Poiché il trattamento dei dati finanziari è collegato a una serie di gravi rischi, le misure di sicurezza dovrebbero essere conseguentemente rigorose.

71. I fornitori di servizi dovrebbero essere tenuti a rispettare norme severe, compresi meccanismi di autenticazione forte del cliente e norme di sicurezza rigorose per i dispositivi tecnici[37]. Sono importanti anche altre procedure, come la verifica delle norme di sicurezza e delle procedure operative contro l'accesso non autorizzato predisposte dai responsabili del trattamento.

6.4 TRASPARENZA E RESPONSABILIZZAZIONE

72. La trasparenza e la responsabilizzazione sono due principi fondamentali del GDPR.

73. Per quanto riguarda la trasparenza (articolo 5, paragrafo 1, lettera a), del GDPR), l'articolo 12 del GDPR specifica che i titolari del trattamento devono adottare misure appropriate per fornire tutte le informazioni di cui agli articoli 13 e 14 del regolamento. Inoltre, a norma dello stesso articolo, le informazioni o le comunicazioni riguardanti il trattamento dei dati personali

devono essere concise, trasparenti, intelligibili e facilmente accessibili. Le informazioni devono essere formulate con un linguaggio semplice e chiaro e devono essere fornite per iscritto "o con altri mezzi, anche, se del caso, con mezzi elettronici". Le linee guida del gruppo di lavoro Articolo 29 sulla trasparenza ai sensi del regolamento 2016/679, approvate dal comitato europeo per la protezione dei dati, forniscono orientamenti specifici riguardanti il rispetto del principio di trasparenza negli ambienti digitali.

74. Secondo le suddette linee guida sulla trasparenza ai sensi del regolamento 2016/679, l'articolo 11 del GDPR dovrebbe essere interpretato come un modo per realizzare un'effettiva minimizzazione dei dati senza ostacolare l'esercizio dei diritti dell'interessato e tale esercizio dovrebbe essere reso possibile con l'ausilio delle ulteriori informazioni fornite dall'interessato. Vi possono essere situazioni in cui il titolare tratta dati personali che non richiedono l'identificazione dell'interessato (ad esempio dati pseudonimizzati). In tali casi, può risultare pertinente anche l'articolo 11, paragrafo 1, dal momento che afferma che il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il GDPR.

75. Per i servizi di cui alla PSD2, l'articolo 13 del GDPR si applica ai dati personali raccolti presso l'interessato, mentre l'articolo 14 si applica qualora i dati personali non siano stati ottenuti presso l'interessato.

76. L'interessato deve essere informato in particolare del periodo di conservazione dei dati personali oppure, se ciò non è possibile, dei criteri utilizzati per determinare tale periodo e, se del caso, dei legittimi interessi perseguiti dal titolare del trattamento o da eventuali terzi. Qualora il trattamento sia basato sul consenso di cui all'articolo 6, paragrafo 1, lettera a), del GDPR o sul consenso esplicito di cui all'articolo 9, paragrafo 2, lettera a), del GDPR, l'interessato deve essere informato dell'esistenza del diritto di revocare il consenso in qualsiasi momento.

77. Il titolare del trattamento deve fornire le informazioni all'interessato, tenendo conto delle specifiche circostanze in cui i dati personali sono trattati. Nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato[38], circostanza che riguarderà probabilmente gli AISP, le informazioni devono essere fornite al più tardi al momento della prima comunicazione all'interessato. Se i dati personali devono essere comunicati a un altro destinatario, le informazioni devono essere fornite al più tardi al momento della prima comunicazione dei dati personali.

78. Per quanto riguarda i servizi di pagamento online, le suddette linee guida chiariscono che i titolari del trattamento possono adottare un approccio stratificato, optando per una combinazione di metodi al fine di assicurare la trasparenza. Si raccomanda in particolare l'impiego di dichiarazioni/informative sulla privacy stratificate per collegare le varie categorie di informazioni da fornire all'interessato, piuttosto che l'inserimento di tutte le informazioni in un'unica informativa su una schermata, così da evitare un sovraccarico di informazioni e garantire nel contempo l'efficacia delle stesse.

79. Le suddette linee guida chiariscono inoltre che i titolari del trattamento possono scegliere di utilizzare strumenti aggiuntivi per fornire informazioni al singolo interessato, come ad esempio i dashboard ("cruscotti di controllo") per la privacy. Un dashboard per la privacy è un punto unico dal quale l'interessato può visualizzare le "informazioni sulla privacy" e gestire le proprie preferenze permettendo o impedendo al titolare del trattamento in questione determinati usi dei dati che lo riguardano[39]. Un dashboard per la privacy potrebbe fornire una panoramica dei prestatori terzi che hanno ottenuto il consenso esplicito dell'interessato, nonché informazioni pertinenti sulla natura e sulla quantità di dati personali cui i prestatori terzi hanno avuto accesso. In linea di principio, l'ASPSP può offrire all'utente la possibilità di revocare uno specifico consenso esplicito a norma della PSD2[40] attraverso la panoramica, negando così a uno o più prestatori terzi l'accesso ai propri conti di pagamento. L'utente potrebbe inoltre chiedere a un ASPSP di negare l'accesso ai propri conti di pagamento a uno o più prestatori terzi specifici[41], in quanto l'utente ha il diritto di (non) avvalersi di un servizio di informazione sui conti. Se i dashboard per la privacy vengono utilizzati per accordare o revocare un consenso esplicito, dovrebbero essere progettati e applicati a norma di legge, evitando in particolare di limitare il diritto dei prestatori terzi di fornire servizi conformemente alla PSD2. A tale riguardo e in conformità delle disposizioni applicabili a norma della PSD2, un prestatore terzo ha la possibilità di ottenere nuovamente il consenso esplicito dell'utente dopo che tale consenso è stato revocato.

80. I principi di responsabilizzazione impongono al titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR, in particolare ai principi fondamentali di protezione dei dati di cui all'articolo 5, paragrafo 1. Tali misure dovrebbero tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi per i diritti e le libertà delle persone fisiche e devono essere riesaminate e aggiornate qualora necessario[42].

6.5 PROFILAZIONE

81. Il trattamento dei dati personali da parte dei prestatori di servizi di pagamento può comportare una "profilazione" ai sensi dell'articolo 4, punto 4), del GDPR. Gli AISP potrebbero ad esempio avvalersi del trattamento automatizzato dei dati personali al fine di valutare taluni aspetti personali relativi a una persona fisica. A seconda delle specificità del servizio, potrebbe essere valutata la situazione finanziaria personale dell'interessato. I servizi di informazione sui conti, che sono prestati su richiesta dell'utente, possono comportare una valutazione approfondita dei dati personali relativi ai conti di pagamento.

82. Il titolare del trattamento deve inoltre essere trasparente nei confronti dell'interessato in merito all'esistenza di un processo decisionale automatizzato, compresa la profilazione. In tali casi il titolare del trattamento deve

fornire informazioni significative sulla logica utilizzata, nonché sull'importanza e sulle conseguenze previste di tale trattamento per l'interessato (articolo 13, paragrafo 2, lettera f), articolo 14, paragrafo 2, lettera g), e considerando 60)[43]. Analogamente, a norma dell'articolo 15 del GDPR, l'interessato ha il diritto di chiedere e ottenere dal titolare del trattamento informazioni in merito all'esistenza di un processo decisionale automatizzato, compresa la profilazione, alla logica utilizzata e alle conseguenze per l'interessato e, in determinate circostanze, ha il diritto di opporsi alla profilazione, indipendentemente dal fatto che abbia luogo un processo decisionale totalmente automatizzato relativo alle persone fisiche[44].

83. In questo contesto rileva inoltre il diritto dell'interessato di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, come previsto dall'articolo 22 del GDPR. Tale norma prevede inoltre, in determinate circostanze, la necessità che il titolare del trattamento attui misure appropriate per tutelare i diritti dell'interessato, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano nel processo decisionale, di esprimere la propria opinione e di contestare la decisione. Come indicato anche al considerando 71 del GDPR, ciò implica, tra l'altro, che gli interessati hanno il diritto di non essere sottoposti a una decisione, come il rifiuto automatico di una domanda di credito online, senza alcun intervento umano[45].

84. Il processo decisionale automatizzato, compresa la profilazione, che comporta l'uso di categorie particolari di dati personali è consentito soltanto se sono soddisfatte le condizioni cumulative di cui all'articolo 22, paragrafo 4, del GDPR:

- è applicabile un'esenzione di cui all'articolo 22, paragrafo 2;
- si applica l'articolo 9, paragrafo 2, lettere a) o g), del GDPR. In entrambi i casi il titolare del trattamento deve adottare misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato[46].

85. Come indicato nelle suddette linee guida, dovrebbero essere rispettati anche i requisiti per l'ulteriore trattamento. I chiarimenti e le indicazioni riguardanti il processo decisionale automatizzato relativo alle persone fisiche e la profilazione forniti dal gruppo di lavoro Articolo 29 nelle linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, approvate dall'EDPB, sono pienamente pertinenti nel contesto dei servizi di pagamento e dovrebbero pertanto essere presi in debita considerazione.

Per il Comitato europeo per la protezione dei dati
La presidente

(Andrea Jelinek)

NOTE

[1] Nel presente documento, i riferimenti agli "Stati membri" sono da intendersi come riferimenti agli "Stati membri del SEE".

[2] Considerando 6 della PSD2.

[3] Poiché la PSD2 è precedente al GDPR, fa ancora riferimento alla direttiva 95/46/CE. L'articolo 94 del GDPR stabilisce che i riferimenti alla direttiva 95/46/CE abrogata si intendono fatti al GDPR.

[4] Considerando 89 della PSD2.

[5] Articolo 1, paragrafo 1, del GDPR.

[6] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche). (GU L 201 del 31.7.2002, pag. 37).

[7] Articolo 94 della direttiva sui servizi di pagamento, ecc.

[8] Regolamento delegato (UE) 2018/389 della Commissione, del 27 novembre 2017, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (Testo rilevante ai fini del SEE), C/2017/7782 (GU L 69 del 13.3.2018, pag. 23) consultabile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018R0389&from=IT.

[9] Un servizio di informazione sui conti è un servizio online che fornisce informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento.

[10] L'articolo 1, paragrafo 1, della PSD2 afferma che la direttiva stabilisce le regole in base alle quali gli Stati membri devono distinguere le seguenti categorie di prestatori di servizi di pagamento:
a) gli enti creditizi quali definiti all'articolo 4, paragrafo 1, punto 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio (1), comprese le relative succursali quali definite al relativo punto 17), se tali succursali sono situate nell'Unione, indipendentemente dal fatto che le sedi centrali di dette succursali siano situate nell'Unione ovvero, conformemente all'articolo 47 della direttiva 2013/36/UE e alla normativa nazionale, al di fuori dell'Unione;
b) gli istituti di moneta elettronica quali definiti all'articolo 2, punto 1), della direttiva 2009/110/CE, comprese – conformemente all'articolo 8 di detta direttiva e al diritto nazionale – le relative succursali qualora queste siano situate nell'Unione e le loro sedi centrali siano situate al di fuori dell'Unione, nella misura in cui i servizi di pagamento prestati da dette succursali siano connessi all'emissione di moneta elettronica;
c) gli uffici postali che hanno il diritto di prestare servizi di pagamento a norma del diritto nazionale;
d) gli istituti di pagamento;
e) la BCE e le banche centrali nazionali ove non agiscano in quanto autorità monetarie o altre autorità pubbliche;
f) gli Stati membri o le rispettive autorità regionali o locali ove non agiscano in quanto autorità pubbliche.

[11] Articolo 4, punto 15), della PSD2.

[12] Articolo 4, punto 16), della PSD2.

[13] A norma dell'articolo 6, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
(a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
(b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
(c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
(d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
(e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
(f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

[14] EDPB, linee guida 2/2019

sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, pag. 8.

[15] Ibidem.

[16] Ibidem, pag. 7.

[17] Ibidem, pag. 10.

[18] Ibidem, pag. 11.

[19] Considerando 47 del GDPR.

[20] Si noti che un esame approfondito della questione riguardante la conformità o meno della direttiva antiriciclaggio alle norme di cui all'articolo 6, paragrafo 4, del GDPR esula dall'oggetto del presente documento.

[21] EDPB, linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, punto 3.

[22] Cfr. anche il parere 15/2011 sulla definizione di consenso (WP 187), pagg. 6-8, e/o il parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE (WP 217), pagg. 9, 10, 13 e 14.

[23] Lettera dell'EDPB relativa alla direttiva PSD2, 5 luglio 2018, pag. 4.

[24] Ciò vale per i servizi da 1 a 7 dell'allegato I della PSD2.

[25] L'articolo 94, paragrafo 2, della PSD2 rientra nel capo 4 "Protezione dei dati".

[26] Gruppo di lavoro Articolo 29, linee guida sulla trasparenza ai sensi del regolamento 2016/679, punto 10 (adottate l'11 aprile 2018) – approvate dall'EDPB.

[27] Gruppo di lavoro Articolo 29, parere 03/2013 sulla limitazione delle finalità (WP 203), pag. 16.

[28] Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, punto 16 (versione per la consultazione pubblica), e parere 03/2013 del gruppo di lavoro Articolo 29 sulla limitazione delle finalità (WP 203), pagg. 15-16.

[29] Il considerando 87 della PSD2 afferma che la direttiva riguarda "solo gli obblighi e le responsabilità contrattuali tra l'utente dei servizi di pagamento e il corrispondente prestatore di servizi di pagamento". I dati dei taciti interessati non rientrano pertanto nell'ambito di applicazione della PSD2.

[30] Occorre prestare particolare attenzione al trattamento dei dati personali finanziari, in quanto il trattamento può comportare un aumento del possibile rischio per i diritti e le libertà delle persone fisiche, secondo le linee guida in materia di valutazione d'impatto sulla protezione dei dati.

[31] Gruppo di lavoro Articolo 29 per la protezione dei dati, linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, WP 251 rev.01, pag. 15.

[32] Ad esempio, al considerando 10 del GDPR si fa riferimento a categorie particolari di dati personali con il termine "dati sensibili".

[33] EDPB, linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, punto 99.

[34] EDPB, linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, punto 32.

[35] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, pag. 29.

[36] Gruppo di lavoro Articolo 29, linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, WP 248 rev.01, approvate dall'EDPB.

[37] Si vedano le norme tecniche di regolamentazione.

[38] Articolo 14, paragrafo 3, lettera b), del GDPR.

[39] Secondo le linee guida del gruppo di lavoro Articolo 29 sulla trasparenza ai sensi del regolamento 2016/679, approvate dall'EDPB, i dashboard per la privacy sono particolarmente utili quando gli interessati usano lo stesso servizio su diversi dispositivi, poiché consentono loro di accedere ai loro dati personali e di controllarli, indipendentemente dal modo in cui utilizzano il servizio. Il fatto che l'interessato possa modificare manualmente le impostazioni sulla privacy tramite un apposito dashboard può inoltre facilitare la personalizzazione della dichiarazione/informativa sulla privacy, che sarà in grado di rispecchiare solo i tipi di trattamento che si verificano per quel particolare interessato.

[40] Cfr. ad esempio il "consenso esplicito" di cui all'articolo 67, paragrafo 2, lettera a), della PSD2.

[41] Cfr. anche EBA/OP/2020/10, punto 45.

[42] Articolo 5, paragrafo 2, e articolo 24 del GDPR.

[43] Linee guida sulla trasparenza ai sensi del regolamento 2016/679, WP 260 rev.01, approvate dall'EDPB.

[44] Gruppo di lavoro Articolo 29, linee guida sul processo de-

cisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, WP 251 rev.01.

[45] Considerando 71 del GDPR.

[46] Gruppo di lavoro Articolo 29, linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, WP 251 rev.01, pag. 24.

Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR Versione 2.0

Adottate il 7 luglio 2021

Cronologia delle versioni

Versione 2.0	7 luglio 2021	Adozione delle linee guida in seguito a consultazione pubblica
Versione 1.0	2 settembre 2020	Adozione delle linee guida per consultazione pubblica

SINTESI

I concetti di titolare del trattamento, di contitolare del trattamento e di responsabile del trattamento svolgono un ruolo fondamentale nell'applicazione del regolamento generale sulla protezione dei dati [GDPR, regolamento (UE) 2016/679)], in quanto stabiliscono chi è il responsabile del rispetto delle diverse norme in materia di protezione dei dati e in che modo gli interessati possono esercitare i propri diritti in concreto. Il significato preciso di tali concetti e i criteri per una corretta interpretazione degli stessi devono essere sufficientemente chiari e coerenti in tutto lo Spazio economico europeo (SEE).

I concetti di titolare del trattamento, di contitolare del trattamento e di responsabile del trattamento sono *funzionali*, in quanto mirano a ripartire le responsabilità in funzione dei ruoli effettivi delle parti, e *autonomi*, nel senso che dovrebbero essere interpretati principalmente ai sensi del diritto dell'UE in materia di protezione dei dati.

Titolare del trattamento

In linea di principio non vi sono limitazioni per quanto concerne la natura dei soggetti che possono assumere il ruolo di titolare del trattamento, tuttavia in pratica è solitamente l'organizzazione in quanto tale e non una persona fisica all'interno dell'organizzazione (come l'amministratore delegato, un dipendente o un membro del consiglio di amministrazione) ad agire in qualità di titolare del trattamento.

Il titolare del trattamento è il soggetto che *decide* in merito a determinati elementi chiave del trattamento stesso. La titolarità può essere definita a norma di legge o può derivare da un'analisi degli elementi di fatto o delle circostanze del caso. Talune attività di trattamento possono essere considerate come naturalmente connesse al ruolo ricoperto da un determinato soggetto (il datore di lavoro rispetto ai dipendenti, l' editore rispetto agli abbonati o un'associazione rispetto ai membri). In molti casi, le condizioni previste da un contratto possono agevolare l'individuazione del titolare del trattamento, sebbene non siano sempre determinanti.

Il titolare stabilisce le finalità e i mezzi del trattamento, ossia il *motivo* e le *modalità* del trattamento. Il titolare del trattamento è chiamato a decidere tanto sulle finalità quanto sui mezzi. Tuttavia, taluni aspetti più prettamente pratici legati all'implementazione del trattamento («mezzi non essenziali») possono essere delegati al responsabile del trattamento. Per essere qualificato come titolare del trattamento non è necessario che tale soggetto abbia accesso effettivo ai dati trattati.

Contitolari del trattamento

La contitolarità di trattamento può configurarsi laddove più di un soggetto sia coinvolto nel trattamento. Il GDPR introduce norme specifiche per i contitolari

del trattamento e definisce un quadro per disciplinare i loro rapporti. Il criterio generale per la sussistenza della contitolarità di trattamento è la partecipazione congiunta di due o più soggetti nella definizione delle finalità e dei mezzi di un'operazione di trattamento. La partecipazione congiunta può assumere la forma di una *decisione comune*, presa da due o più soggetti, o può derivare dalle *decisioni convergenti* di due o più soggetti, qualora tali decisioni si integrino vicendevolmente e siano necessarie affinché il trattamento abbia luogo così da esplicare un effetto tangibile sulla definizione delle finalità e dei mezzi del trattamento. Un criterio importante è che il trattamento non sarebbe possibile senza la partecipazione di entrambi i soggetti, nel senso che i trattamenti svolti da ciascun soggetto sono tra loro indissociabili, ovverosia indissolubilmente legati. La partecipazione congiunta comprende, da un lato, la determinazione delle finalità e, dall'altro, la determinazione dei mezzi.

Responsabile del trattamento

Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organo che tratta dati personali per conto del titolare del trattamento. Due condizioni sono indispensabili per configurare il ruolo di responsabile del trattamento: essere un soggetto distinto rispetto al titolare del trattamento e trattare dati personali per conto del titolare del trattamento.

Al responsabile del trattamento non è consentito trattare i dati in modo diverso rispetto a quanto indicato nelle istruzioni del titolare. Tuttavia, le istruzioni del titolare del trattamento possono lasciare un certo margine di discrezionalità su come servirne al meglio gli interessi, consentendo al responsabile del trattamento di avvalersi dei mezzi tecnici e organizzativi più idonei. Ciononostante, un responsabile del trattamento viola il GDPR qualora non si limiti a trattare i dati in base alle istruzioni del titolare del trattamento e inizi a definire mezzi e finalità propri. Il responsabile del trattamento sarà pertanto considerato titolare rispetto a tale ultimo trattamento e può essere soggetto a sanzioni qualora non si limiti a trattare i dati in base alle istruzioni impartite dal titolare del trattamento.

Rapporto tra titolare e responsabile del trattamento

Il titolare del trattamento deve avvalersi unicamente di responsabili del trattamento che presentino garanzie sufficienti per l'attuazione di misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR. Gli elementi di cui tenere conto potrebbero essere le conoscenze specialistiche del responsabile del trattamento (ad esempio, le competenze tecniche in materia di misure di sicurezza e di violazione dei dati), il grado di affidabilità, le risorse di cui dispone il responsabile e l'adesione di quest'ultimo a un codice di condotta o a un meccanismo di certificazione riconosciuti.

Qualsivoglia trattamento di dati personali da parte di un responsabile del trattamento deve essere disciplinato da un contratto o da un atto giuridico di altra natura, redatto per iscritto, anche in formato elettronico, con carattere di vincolatività. Il titolare e il responsabile del trattamento possono negoziare un contratto

specifico, comprensivo di tutti gli elementi obbligatori, oppure basarsi, in tutto o in parte, su clausole contrattuali tipo.

Il GDPR elenca gli elementi che devono figurare nell'accordo di trattamento, il quale tuttavia non dovrebbe limitarsi a ribadire le disposizioni del GDPR; piuttosto, tale accordo dovrebbe disciplinare in modo più specifico e concreto come saranno soddisfatti i requisiti applicabili e quale sia il livello di sicurezza richiesto per il trattamento dei dati personali oggetto dell'accordo stesso.

Rapporto tra contitolari del trattamento

I contitolari del trattamento stabiliscono e concordano in modo trasparente le rispettive responsabilità per quanto concerne l'adempimento degli obblighi di cui al GDPR. La determinazione delle rispettive responsabilità deve riguardare in particolare l'esercizio dei diritti degli interessati e gli obblighi di informazione. Inoltre, la ripartizione delle responsabilità dovrebbe riguardare altri obblighi in capo al titolare del trattamento, quali il rispetto dei principi generali in materia di protezione dei dati, la base giuridica, le misure di sicurezza, l'obbligo di notifica di violazione dei dati, le valutazioni d'impatto sulla protezione dei dati, il ricorso a responsabili del trattamento, i trasferimenti verso paesi terzi e i contatti con gli interessati e le autorità di controllo.

Ciascun contitolare è tenuto a disporre di una base giuridica per il trattamento e a garantire che i dati non siano oggetto di ulteriore trattamento secondo modalità incompatibili con le finalità per le quali sono stati inizialmente raccolti dal titolare che li comunica.

Il GDPR non specifica la forma giuridica dell'accordo tra contitolari del trattamento. Ai fini della certezza del diritto e per garantire il rispetto dei principi di trasparenza e responsabilizzazione, l'EDPB raccomanda che l'accordo sia stipulato sotto forma di documento vincolante, ossia di contratto o di atto giuridico vincolante di altra natura, ai sensi del diritto dell'UE o dello Stato membro cui sono soggetti i titolari del trattamento.

L'accordo riflette debitamente i ruoli e i rapporti rispettivi dei contitolari di trattamento nei confronti degli interessati e i suoi elementi essenziali sono messi a disposizione dell'interessato.

Indipendentemente dai termini dell'accordo, gli interessati hanno facoltà di esercitare i propri diritti nei confronti di e contro ciascuno dei contitolari del trattamento. Le autorità di controllo non sono vincolate dalle condizioni dell'accordo né per quanto concerne la qualifica di contitolari né per quanto concerne i punti di contatto designati.

Indice

INTRODUZIONE

PARTE I – CONCETTI

1 OSSERVAZIONI GENERALI

2 DEFINIZIONE DI TITOLARE DEL TRATTAMENTO
- 2.1 Definizione di titolare del trattamento
  - 2.1.1 «Persona fisica o giuridica, autorità pubblica, servizio o altro organismo»
  - 2.1.2 «Determina»
  - 2.1.3 «Singolarmente o insieme ad altri»
  - 2.1.4 «Finalità e mezzi»
  - 2.1.5 «Del trattamento dei dati personali»

3 DEFINIZIONE DI CONTITOLARI DEL TRATTAMENTO
- 3.1 Definizione di contitolari del trattamento
- 3.2 Esistenza di una contitolarità del trattamento
  - 3.2.1 Considerazioni generali
  - 3.2.2 Valutazione della partecipazione congiunta
  - 3.2.3 Situazioni in cui non sussiste contitolarità del trattamento

4 DEFINIZIONE DI RESPONSABILE DEL TRATTAMENTO

5 DEFINIZIONE DI TERZO/DESTINATARIO

PARTE II – CONSEGUENZE DERIVANTI DAI DIVERSI RUOLI ATTRIBUITI

1 RAPPORTO TRA TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO
- 1.1 Scelta del responsabile del trattamento
- 1.2 Forma del contratto o dell'atto giuridico di altra natura
- 1.3 Contenuto del contratto o altro atto giuridico
  - 1.3.1 Obbligo del responsabile del trattamento di trattare i dati solo su istruzione documentata del titolare del trattamento (articolo 28, paragrafo 3, lettera a) del GDPR)
  - 1.3.2 Obbligo del responsabile del trattamento di garantire che le persone autorizzate a trattare i dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza (articolo 28, paragrafo 3, lettera b) del GDPR)
  - 1.3.3 Obbligo del responsabile del trattamento di adottare tutte le

misure richieste a norma dell'articolo 32 (articolo 28, paragrafo 3, lettera c) del GDPR)

1.3.4 Obbligo del responsabile del trattamento di rispettare le condizioni di cui all'articolo 28, paragrafo 2, e all'articolo 28, paragrafo 4, per ricorrere a un altro responsabile del trattamento (articolo 28, paragrafo 3, lettera d) del GDPR)

1.3.5 Obbligo del responsabile del trattamento di assistere il titolare del trattamento nell'adempimento dell'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato (articolo 28, paragrafo 3, lettera e), del GDPR)

1.3.6 Obbligo del responsabile del trattamento di assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 (articolo 28, paragrafo 3, lettera f), del GDPR)

1.3.7 Obbligo del responsabile del trattamento, al termine della relativa attività, di cancellare o restituire, su scelta del titolare del trattamento, tutti i dati personali al titolare del trattamento e cancellare le copie esistenti (articolo 28, paragrafo 3, lettera g), del GDPR)

1.3.8 Obbligo del responsabile del trattamento di mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato (articolo 28, paragrafo 3, lettera h), del GDPR)

1.4 Istruzioni che violano la normativa in materia di protezione dei dati

1.5 Responsabile del trattamento che determina le finalità e i mezzi del trattamento

1.6 Sub-responsabili

2 CONSEGUENZE DELLA CONTITOLARITÀ DEL TRATTAMENTO

2.1 Determinazione in modo trasparente delle responsabilità rispettive dei contitolari del trattamento per quanto riguarda il rispetto degli obblighi previsti dal GDPR

2.2 Obbligo di effettuare la ripartizione delle responsabilità mediante un accordo

2.2.1 Forma dell'accordo

2.2.2 Obblighi nei confronti degli interessati

2.3 Obblighi nei confronti delle autorità di protezione dei dati

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito il «GDPR» o «il regolamento»),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo n. 37 dello stesso, modificati dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

visti gli articoli 12 e 22 del proprio regolamento interno,

considerando che il lavoro preparatorio delle presenti linee guida ha comportato la raccolta di contributi da parte delle parti interessate, sia per iscritto che in occasione di un evento dedicato alle stesse, al fine di individuare le sfide più urgenti,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

INTRODUZIONE

1. Il presente documento è inteso a fornire orientamenti sui concetti di titolare del trattamento e di responsabile del trattamento, ai sensi delle norme del GDPR relative alle definizioni di cui all'articolo 4 e delle disposizioni relative agli obblighi di cui al capo IV. L'obiettivo principale è chiarire il significato dei concetti nonché i diversi ruoli e la ripartizione delle responsabilità tra i soggetti in questione.

2. Il concetto di titolare del trattamento e la sua interazione con quello di responsabile del trattamento svolgono un ruolo fondamentale nell'applicazione del GDPR, in quanto determinano chi è responsabile del rispetto delle diverse norme in materia di protezione dei dati e in che modo gli interessati possono esercitare i propri diritti in concreto. Il GDPR introduce esplicitamente il principio di responsabilizzazione, nel senso che il titolare del trattamento è competente per il rispetto dei principi relativi al trattamento dei dati personali di cui all'articolo 5 ed è in grado di comprovarlo. Inoltre, il GDPR introduce norme più specifiche sul ricorso a uno o più responsabili del trattamento, e talune disposizioni in materia di trattamento dei dati personali riguardano non solo i titolari ma anche i responsabili del trattamento.

3. È pertanto di fondamentale importanza che il significato preciso di tali concetti e i criteri per il loro corretto utilizzo siano sufficientemente chiari e condivisi in tutta l'Unione europea e nel SEE.

4. Il gruppo di lavoro Articolo 29 ha pubblicato orientamenti sui concetti di titolare del trattamento e responsabile del trattamento [rispettivamente «responsabile» e «incaricato» nel parere 1/2010 (WP 169)][2], allo scopo di fornire chiarimenti ed esempi concreti in merito. Dall'entrata in vigore del GDPR ci si è interrogati più volte sulla misura in cui quest'ultimo avesse modificato i concetti di titolare del trattamento e di responsabile del trattamento e i rispettivi ruoli. In particolare, sono stati sollevati interrogativi sul merito e sulle implicazioni del concetto di contitolarità di trattamento (ad esempio, ai sensi dell'articolo 26 del GDPR) e sugli obblighi specifici per i responsabili del trattamento di cui al capo IV (ad esempio, ai sensi dell'articolo 28 del GDPR). Pertanto, e poiché riconosce che l'applicazione concreta dei concetti richiede ulteriori chiarimenti, l'EDPB ritiene necessario fornire orientamenti più articolati e specifici, al fine di garantire un approccio coerente e armonizzato in tutta l'UE e nel SEE. Le presenti linee guida sostituiscono il precedente parere del gruppo di lavoro Articolo 29 su tali concetti (WP 169).

5. Nella parte I, le presenti linee guida esaminano le definizioni dei diversi concetti di titolare del trattamento, contitolari di trattamento, responsabile del trattamento e terzo/destinatario. Nella parte II sono forniti ulteriori orientamenti sulle conseguenze legate ai diversi ruoli svolti dal titolare del trattamento, dai contitolari di trattamento e dal responsabile del trattamento.

PARTE I – CONCETTI

OSSERVAZIONI GENERALI

6. L'articolo 5, paragrafo 2, del GDPR introduce esplicitamente il principio di responsabilizzazione. Ciò significa che:

- il titolare del trattamento è *responsabile del rispetto* dei principi di cui all'articolo 5, paragrafo 1, del GDPR;
- il titolare del trattamento è in grado di *dimostrare il rispetto* dei principi di cui all'articolo 5, paragrafo 1, del GDPR.

Questo principio è stato descritto in un parere del gruppo di lavoro Articolo 29[3] e non sarà trattato in dettaglio nelle presenti linee guida.

7. L'obiettivo di integrare il principio di responsabilizzazione nel GDPR e di renderlo un principio centrale era volto a sottolineare che i titolari del trattamento devono attuare misure adeguate ed efficaci ed essere in grado di dimostrare la conformità al regolamento[4].

8. L'articolo 24 specifica ulteriormente il principio di responsabilizzazione, prevedendo l'obbligo in capo al titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato in conformità del GDPR. Tali misure sono riesaminate e aggiornate, se del caso. Anche l'articolo 28, che stabilisce gli obblighi del titolare del trattamento laddove si avvalga di un responsabile del trattamento, richiama il principio di responsabilizzazione.

9. Il principio di responsabilizzazione si rivolge direttamente al titolare del trattamento. Tuttavia, talune norme più specifiche, come quelle sui poteri delle autorità di controllo di cui all'articolo 58, sono rivolte sia ai titolari sia ai responsabili del trattamento. Entrambi possono essere oggetto di sanzioni in caso di inadempimento degli obblighi cui sono soggetti ai sensi del GDPR ed entrambi sono direttamente responsabili nei confronti delle autorità di controllo, in virtù dell'obbligo di conservare e fornire la documentazione adeguata su richiesta, di cooperare in caso di indagini e di ottemperare ai provvedimenti amministrativi. Al contempo, occorre rammentare che i responsabili del trattamento devono attenersi sempre alle istruzioni del titolare del trattamento e agire unicamente in base a esse.

10. Il principio di responsabilizzazione, insieme alle altre norme che disciplinano in modo più specifico le modalità di adempimento del GDPR e la ripartizione delle responsabilità, rende pertanto necessario definire i diversi ruoli dei vari soggetti coinvolti in un'attività di trattamento di dati personali.

11. Un'osservazione di natura generale riguardante i concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR è che tali concetti non hanno subito cambiamenti rispetto alla direttiva 95/46/CE e che, nel complesso, i criteri per l'attribuzione dei vari ruoli restano immutati.

12. Quelli di titolare del trattamento e di responsabile del trattamento sono con-

cetti *funzionali*: mirano a ripartire le responsabilità in funzione dei ruoli effettivamente svolti[5]. Ciò implica che lo status giuridico di un soggetto in quanto «titolare del trattamento» o «responsabile del trattamento» deve, in linea di principio, essere determinato dalle attività effettivamente svolte in una situazione specifica, piuttosto che dalla sua designazione formale in quanto «titolare del trattamento» o «responsabile del trattamento» (ad esempio in un contratto)[6]. Ciò significa che la ripartizione dei ruoli dovrebbe, di norma, derivare da un'analisi degli elementi di fatto o delle circostanze del caso e, in quanto tale, non è negoziabile.

13. I concetti di titolare del trattamento e di responsabile del trattamento sono altresì concetti *autonomi*, nel senso che, sebbene fonti giuridiche esterne possano contribuire all'individuazione del titolare del trattamento, la loro interpretazione dovrebbe basarsi principalmente sul diritto dell'UE in materia di protezione dei dati. Il concetto di titolare del trattamento non dovrebbe essere confuso con altri concetti, talvolta contrastanti o coincidenti, propri di altri campi del diritto, come quello di autore o di titolare dei diritti in materia di proprietà intellettuale o di diritto della concorrenza.

14. Poiché l'obiettivo di fondo nell'attribuzione del ruolo di titolare del trattamento è garantire il rispetto del principio di responsabilizzazione e una protezione efficace e completa dei dati personali, il concetto di «titolare del trattamento» dovrebbe essere interpretato in modo sufficientemente estensivo, favorendo il più possibile una tutela efficace e completa degli interessati[7], in modo da garantire la piena efficacia del diritto dell'UE in materia di protezione dei dati, evitare lacune e prevenire elusioni potenziali delle norme, senza sminuire, al contempo, il ruolo del responsabile del trattamento.

2. DEFINIZIONE DI TITOLARE DEL TRATTAMENTO

2.1 DEFINIZIONE DI TITOLARE DEL TRATTAMENTO

15. L'articolo 4, paragrafo 7, del GDPR definisce come titolare del trattamento

*«**la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali**; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere **stabiliti dal diritto dell'Unione o degli Stati membri**».*

16. La definizione di titolare del trattamento prevede cinque elementi principali, che saranno analizzati separatamente ai fini delle presenti linee guida. Questi elementi sono:

- «la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo»
- «determina»
- «singolarmente o insieme ad altri»

- «le finalità e i mezzi»
- «del trattamento dei dati personali».

2.1.1 «PERSONA FISICA O GIURIDICA, AUTORITÀ PUBBLICA, SERVIZIO O ALTRO ORGANISMO»

17. Il primo elemento costitutivo si riferisce alla natura soggettiva del titolare del trattamento. Ai sensi del GDPR, il titolare del trattamento può essere «*una persona fisica o giuridica, un'autorità pubblica, un servizio o un altro organismo*». Ciò significa che, in linea di principio, non vi sono limitazioni riguardo alle caratteristiche soggettive del titolare del trattamento. Potrebbe trattarsi di un'organizzazione, ma anche di un singolo o di un gruppo di persone[8]. In pratica, tuttavia, è solitamente l'organizzazione in quanto tale e non una persona fisica all'interno dell'organizzazione (come l'amministratore delegato, un dipendente o un membro del consiglio di amministrazione) ad agire in qualità di titolare del trattamento ai sensi del GDPR. Per quanto riguarda il trattamento all'interno di un gruppo di società, occorre prestare particolare attenzione alla questione se uno stabilimento possa agire in qualità di titolare o di responsabile del trattamento, ad esempio quando tratta dati per conto della società controllante.
18. Talvolta le società e gli organismi pubblici designano una persona specifica quale responsabile dell'esecuzione dell'attività di trattamento. Anche se viene designata una persona fisica specifica per garantire il rispetto delle norme in materia di protezione dei dati, tale persona non sarà il titolare del trattamento, ma agirà per conto del soggetto giuridico (società o organismo pubblico) che risponderà in ultima istanza, in caso di violazione delle norme, in qualità di titolare del trattamento. Nella stessa ottica, anche se un determinato dipartimento o unità all'interno di un'organizzazione ha la responsabilità operativa di garantire la conformità di determinate attività di trattamento, ciò non significa che tale dipartimento o unità (anziché l'organizzazione nel suo insieme) assuma il ruolo di titolare del trattamento.

> Esempio
>
> Il dipartimento marketing della società ABC lancia una campagna pubblicitaria per promuovere i suoi prodotti. Il dipartimento decide in merito alla natura della campagna, ai mezzi da utilizzare (e-mail, social media...), ai clienti ai quali rivolgersi e ai dati da utilizzare per ottenere il miglior risultato possibile. Anche se il dipartimento marketing ha agito con notevole indipendenza, in linea di principio la società ABC sarà considerata titolare del trattamento, visto che la campagna pubblicitaria è avviata da tale società e si svolge nell'ambito delle sue attività commerciali e per le sue finalità.

19. In linea di principio, si può presumere che qualsivoglia trattamento di dati

personali da parte dei dipendenti nell'ambito delle attività di un'organizzazione abbia luogo sotto il controllo di quest'ultima[9]. In circostanze eccezionali, tuttavia, può avvenire che un dipendente decida di utilizzare i dati personali per finalità proprie, andando così illegittimamente oltre l'autorità conferitagli (ad esempio per costituire una propria società o per fini analoghi). Spetta pertanto all'organizzazione, in quanto titolare del trattamento, assicurarsi che siano poste in essere misure tecniche e organizzative adeguate, ivi comprese, ad esempio, la formazione e l'informazione dei dipendenti, per garantire la conformità al GDPR[10].

2.1.2 «DETERMINA»

20. Il secondo elemento costitutivo del concetto di titolare del trattamento si riferisce all'influenza di tale soggetto sul trattamento stesso, in virtù di un esercizio del potere decisionale. Il titolare del trattamento è un soggetto che decide taluni elementi chiave del trattamento. Tale titolarità può essere definita a norma di legge o può derivare da un'analisi degli elementi di fatto o delle circostanze del caso. Occorre studiare le specifiche operazioni di trattamento in questione e capire chi le determina, esaminando in primo luogo le seguenti questioni: *«Perché il trattamento ha luogo?» e «Chi ha deciso che il trattamento debba avvenire per una determinata finalità?»*.

Circostanze che danno luogo alla funzione di controllo

21. Appurato che quello di titolare del trattamento è un concetto funzionale, esso si basa pertanto su un'**analisi fattuale piuttosto che formale**. Per agevolare l'analisi possono essere utilizzati alcuni criteri guida e ipotesi pratiche per guidare e semplificare il processo. Nella maggior parte dei casi, il «soggetto decisore» può essere individuato facilmente e chiaramente sulla base di determinate circostanze giuridiche e/o fattuali dalle quali si può normalmente dedurre l'«influenza», a meno che altri elementi depongano in senso contrario. Si possono distinguere due categorie di situazioni: 1) titolarità derivante da *disposizioni giuridiche*; 2) titolarità derivante da un'*influenza concreta*.

1) *Titolarità derivante da disposizioni giuridiche*

22. Vi sono casi in cui la titolarità può essere ricavata dalla competenza espressamente conferita per legge, ad esempio quando il titolare del trattamento o i criteri specifici per la sua designazione sono determinati dal diritto nazionale o dell'Unione. Infatti, l'articolo 4, paragrafo 7, stabilisce che «*quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*». Mentre l'articolo 4, paragrafo 7, fa riferimento unicamente al «titolare del trattamento» al singolare, l'EDPB ritiene che il diritto dell'Unione o degli Stati membri possa anche designare più titolari del trattamento, eventualmente anche in qualità di contitolari.

23. Il fatto che la titolarità del trattamento sia stata definita specificamente per legge sarà determinante per stabilire chi agisce in quanto titolare. Ciò pre-

suppone che il legislatore abbia designato come titolare del trattamento un soggetto che è effettivamente in grado di esercitare un controllo. La legislazione nazionale di taluni paesi prevede che le autorità pubbliche siano responsabili del trattamento dei dati personali nell'ambito delle rispettive competenze.

24. Tuttavia, più comunemente, anziché designare direttamente il titolare del trattamento o stabilire i criteri per la sua designazione, la legge definisce un compito o impone l'obbligo di raccogliere e trattare determinati dati. In tali casi, la finalità del trattamento è spesso determinata per legge. Il titolare del trattamento è di norma il soggetto cui la legge demanda la realizzazione di tale finalità, di tale funzione pubblica. Ciò sarebbe il caso, ad esempio, laddove un soggetto cui sono affidati determinati compiti pubblici (ad es., prestazioni previdenziali), che non possono essere assolti senza raccogliere almeno un certo numero di dati personali, istituisca una banca dati o un registro per svolgere detta funzione pubblica. In tal caso, la legge stabilisce, pur se indirettamente, chi è il titolare del trattamento. Più in generale, la legge può altresì imporre, a soggetti pubblici o privati, l'obbligo di conservare o fornire determinati dati. Di norma, tali soggetti sarebbero pertanto considerati titolari del trattamento necessario per l'adempimento dell'obbligo in questione.

Esempio: disposizioni giuridiche

La legislazione nazionale del paese A prevede l'obbligo per le autorità comunali di erogare prestazioni sociali quali versamenti mensili ai cittadini in base alla loro situazione finanziaria. Per effettuare tali pagamenti, l'amministrazione comunale deve acquisire ed elaborare dati sulla situazione finanziaria dei richiedenti. Anche se non è previsto esplicitamente dalla legge, le autorità comunali sono i titolari di tale trattamento in virtù, implicitamente, delle disposizioni giuridiche.

2) *Titolarità derivante da un'influenza concreta*

25. In assenza di titolarità derivante da disposizioni giuridiche, la qualifica di titolare del trattamento deve essere stabilita sulla base di una valutazione delle circostanze concrete del trattamento. Occorre prendere in considerazione tutte le circostanze di fatto pertinenti al fine di stabilire se uno specifico soggetto eserciti un'influenza determinante sul trattamento dei dati personali in questione.

26. La necessità di una valutazione fattuale significa anche che la titolarità di un trattamento non deriva dalle caratteristiche soggettive di chi tratta i dati, ma dalle attività concretamente svolte da tale soggetto in un contesto specifico. In altre parole, uno stesso soggetto può agire contemporaneamente in qualità di titolare del trattamento per determinate operazioni di trattamento, e in qualità di responsabile del trattamento per altre operazioni; inoltre, la qualifica di titolare o di responsabile del trattamento va valutata in relazione a ciascuna specifica attività di trattamento dei dati.

27. In pratica, talune operazioni di trattamento possono essere considerate come intrinseche al ruolo o alle attività di un determinato soggetto e, in ultima analisi, tali da comportare responsabilità dal punto di vista della protezione dei dati. Ciò può essere dovuto a disposizioni giuridiche di natura più generale o a una prassi giuridica consolidata in singoli settori (diritto civile, commerciale, del lavoro, ecc.). In tal caso, l'esistenza di determinati ruoli tradizionali e di determinate competenze professionali che, di norma, comportano specifiche responsabilità contribuirà a individuare il titolare del trattamento. Si pensi agli esempi seguenti: un datore di lavoro in relazione al trattamento dei dati personali relativi ai propri dipendenti; un editore che tratta i dati personali degli abbonati; un'associazione che tratta i dati personali riguardanti i soci o collaboratori. Quando un soggetto tratta dati personali nell'ambito delle sue interazioni con i propri dipendenti, clienti o soci, tale soggetto, di norma, determina la finalità e i mezzi relativi al trattamento e agisce pertanto in qualità di titolare del trattamento stesso ai sensi del GDPR.

Esempio: studi legali

La società ABC si rivolge a uno studio legale per rappresentarla in una controversia. Per svolgere tale compito, lo studio legale è tenuto a trattare i dati personali relativi alla causa. Il trattamento dei dati personali è motivato dal mandato dello studio legale di rappresentare il cliente in tribunale. Detto mandato, tuttavia, non riguarda specificamente il trattamento dei dati personali. Lo studio legale agisce con un grado significativo di indipendenza, ad esempio nel decidere quali informazioni utilizzare e come utilizzarle e non vi sono istruzioni della società cliente in merito al trattamento dei dati personali. Il trattamento effettuato dallo studio per svolgere il compito di rappresentante legale della società è pertanto legato al ruolo funzionale dello studio stesso, che deve essere considerato titolare del trattamento.

Esempio: operatori di telecomunicazioni[11]

La fornitura di un servizio di comunicazione elettronica, come la posta elettronica, comporta il trattamento di dati personali. Il fornitore di tali servizi sarà di norma considerato titolare del trattamento dei dati personali necessari per il funzionamento del servizio in quanto tale (ad esempio, dati relativi al traffico e alla fatturazione). Se l'unica finalità e ruolo del fornitore è quello di consentire la trasmissione di messaggi di posta elettronica, il fornitore non sarà considerato titolare del trattamento per quanto riguarda i dati personali contenuti nel messaggio stesso. Il titolare del trattamento dei dati personali contenuti nel messaggio è di norma la persona da cui proviene il messaggio, piuttosto che il prestatore di servizi che offre il servizio di trasmissione.

28. In molti casi, l'analisi delle clausole contrattuali che disciplinano i rapporti tra le diverse parti coinvolte può facilitare l'individuazione del soggetto (o dei soggetti) che opera(no) in qualità di titolare del trattamento. Anche se il contratto non stabilisce chi è il titolare del trattamento, esso può contenere elementi sufficienti per desumere chi decide in merito alle finalità e ai mezzi del trattamento. Può anche accadere che il contratto preveda un'indicazione esplicita sull'identità del titolare del trattamento. Se non sussiste motivo di dubitare che ciò rispecchi fedelmente la realtà, niente vieta di attenersi alle previsioni del contratto. Tuttavia, queste ultime non sono determinanti in modo assoluto, poiché altrimenti le parti potrebbero attribuire le responsabilità a proprio piacimento. Non è possibile assumere il ruolo di titolare del trattamento né esimersi dagli obblighi in capo al titolare del trattamento semplicemente redigendo il contratto in un determinato modo, laddove ciò non corrisponda alle circostanze di fatto.
29. Se una parte decide di fatto le finalità e le modalità del trattamento di dati personali, essa sarà il titolare del trattamento anche laddove un contratto la indichi come responsabile di tale trattamento. Analogamente, non è sufficiente che un contratto designi una parte come «subappaltatore» affinché tale parte contrattuale sia considerata responsabile del trattamento ai sensi della normativa in materia di protezione dei dati[12].
30. In linea con l'approccio fattuale, il termine «determina» significa che il titolare del trattamento è il soggetto che esercita effettivamente un'influenza determinante sulle finalità e sui mezzi del trattamento stesso. Di norma, un contratto che disciplini il trattamento di dati definisce la parte che decide sul trattamento (titolare del trattamento) e la parte che opera secondo specifiche istruzioni (responsabile del trattamento). Anche se il responsabile del trattamento offre un servizio definito in via preliminare in modo specifico, al titolare del trattamento deve essere messa a disposizione una descrizione dettagliata di tale servizio e spetta al titolare adottare la decisione finale con cui si approvano le modalità di esecuzione del trattamento nonché chiedere eventuali modifiche. Inoltre, il responsabile del trattamento non può modificare successivamente gli elementi essenziali dello stesso senza l'approvazione del titolare del trattamento.

Esempio: servizio standardizzato di archiviazione su cloud

Un grande fornitore di servizi di archiviazione su cloud offre ai propri clienti la possibilità di archiviare volumi ingenti di dati personali. Il servizio è completamente standardizzato e i clienti hanno scarsa o nessuna capacità di personalizzarlo. I termini contrattuali sono stabiliti e redatti unilateralmente dal fornitore di servizi cloud e forniti al cliente in un'ottica di «prendere o lasciare». La società X decide di avvalersi del fornitore di servizi cloud per archiviare dati personali relativi ai propri clienti. La società X continuerà a essere considerata titolare del trattamento, alla luce della sua decisione di avvalersi di questo fornitore specifico di servizi cloud per trattare dati personali per le proprie finalità. Nella misura

in cui il fornitore di servizi cloud non tratti i dati personali per le proprie finalità e li archivi esclusivamente per conto dei propri clienti e conformemente alle istruzioni, il fornitore di servizi sarà considerato responsabile del trattamento.

2.1.3 «SINGOLARMENTE O INSIEME AD ALTRI»

31. L'articolo 4, paragrafo 7, riconosce che le «finalità e i mezzi» del trattamento possono essere determinati da più di un soggetto. Inoltre, prevede che il titolare del trattamento sia il soggetto che «singolarmente o insieme ad altri» determina le finalità e i mezzi del trattamento. Ciò significa che più soggetti possono agire in qualità di titolare per un medesimo trattamento e che a ciascuno di essi si applicano pertanto le pertinenti disposizioni in materia di protezione dei dati. Analogamente, un soggetto può essere titolare del trattamento anche laddove non adotti tutte le decisioni in merito alle finalità e ai mezzi. I criteri della contitolarità del trattamento e la misura in cui due o più soggetti esercitano congiuntamente il controllo possono assumere forme diverse, come chiarito di seguito[13].

2.1.4 «FINALITÀ E MEZZI»

32. Il quarto elemento costitutivo della definizione di titolare del trattamento fa riferimento all'oggetto dell'influenza esercitata dal titolare stesso, vale a dire «finalità e mezzi» del trattamento. Ciò rappresenta la parte sostanziale del concetto di titolare del trattamento: quali elementi dovrebbero essere definiti da un soggetto affinché questi possa essere considerato titolare del trattamento.

33. I dizionari definiscono la «finalità» come «un risultato atteso o al quale tendono le azioni pianificate» e «mezzi» come «la modalità con la quale si ottiene un risultato o si raggiunge un fine».

34. Il GDPR stabilisce che i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo che non sia incompatibile con tali finalità. La determinazione delle «finalità» del trattamento e dei «mezzi» per conseguirle riveste pertanto particolare importanza.

35. Determinare le finalità e i mezzi equivale a decidere, rispettivamente, il «perché» e il «come» del trattamento[14]: data un'operazione di trattamento specifica, il titolare del trattamento è il soggetto che ha determinato il *perché* del trattamento (ovverosia «a quale fine» o «per che cosa» viene svolto) e come tale obiettivo è raggiunto (ovverosia quali mezzi sono impiegati per conseguirlo). Una persona fisica o giuridica che esercita tale influenza sul trattamento dei dati personali partecipa alla determinazione delle finalità e dei mezzi dello stesso trattamento, conformemente alla definizione di cui all'articolo 4, paragrafo 7, del GDPR[15].

36. Il titolare del trattamento deve decidere in merito alla finalità e ai mezzi del trattamento come descritto di seguito. Di conseguenza, il titolare del trattamento non può limitarsi alla sola determinazione della finalità: deve anche prendere decisioni in merito ai mezzi del trattamento. Per contro, la parte che agisce in qualità di responsabile del trattamento non può in alcun caso determinarne la finalità.

37. In pratica, se un titolare incarica un responsabile del trattamento di effettuare il trattamento per suo conto, ciò significa spesso che il responsabile del trattamento è in grado di adottare autonomamente determinate decisioni sulle modalità di effettuazione del trattamento in oggetto. L'EDPB riconosce la sussistenza di un certo margine di manovra affinché anche il responsabile del trattamento possa prendere decisioni in relazione al trattamento. In quest'ottica, è necessario fornire orientamenti rispetto **al grado di influenza esercitata** sulla definizione del «perché» e del «come» che comporta l'attribuzione a un soggetto della qualifica di titolare del trattamento nonché rispetto alla misura in cui un responsabile del trattamento possa adottare decisioni in autonomia.

38. Quando un soggetto determina chiaramente le finalità e i mezzi, affidando a un diverso soggetto attività di trattamento che consistono nell'esecuzione delle sue istruzioni dettagliate, la situazione è chiara e non vi sono dubbi che tale diverso soggetto debba essere considerato responsabile del trattamento, mentre il primo è il titolare del trattamento.

Mezzi essenziali rispetto a mezzi non essenziali

39. La questione è dove tracciare la linea di demarcazione tra le decisioni riservate al titolare del trattamento e quelle che possono essere lasciate a discrezione del responsabile del trattamento. Le decisioni sulla finalità del trattamento sono chiaramente sempre di competenza del titolare del trattamento.

40. Per quanto concerne la definizione dei mezzi, si può operare una distinzione tra mezzi essenziali e non essenziali. I «mezzi essenziali» sono tradizionalmente e intrinsecamente riservati al titolare del trattamento. Mentre i mezzi non essenziali possono essere determinati anche dal responsabile del trattamento, i mezzi essenziali sono determinati necessariamente dal titolare del trattamento. Per «mezzi essenziali» si intendono i mezzi strettamente legati alla finalità e alla portata del trattamento, tra cui il tipo di dati personali trattati («*quali dati sono trattati?*»), la durata del trattamento («*per quanto tempo sono trattati?*»), le categorie di destinatari («*chi vi ha accesso?*») e le categorie di interessati («*i dati personali di quali individui sono oggetto di trattamento?*»). Insieme alla finalità del trattamento, i mezzi essenziali sono inoltre strettamente connessi alla liceità, necessità e proporzionalità del trattamento stesso. I «mezzi non essenziali» riguardano aspetti più pratici legati all'esecuzione del trattamento, quali la scelta di un particolare tipo di hardware o di software o le misure di sicurezza specifiche in merito alle quali può decidere il responsabile del trattamento.

Esempio: gestione delle buste paga

Il datore di lavoro A assume un'altra società per gestire il pagamento degli stipendi ai propri dipendenti, impartendo istruzioni chiare su chi pagare, sugli importi, entro quale data, a quale banca, per quanto tempo i dati sono archiviati, quali dati comunicare all'amministrazione fiscale, ecc. In tal caso, il trattamento dei dati è effettuato affinché la società A eroghi gli stipendi ai dipendenti e il responsabile delle buste paga non può utilizzare i dati per finalità proprie. Il modo in cui quest'ultimo dovrebbe effettuare il trattamento è sostanzialmente definito in modo chiaro e rigoroso. Tuttavia, il responsabile delle buste paga può decidere su talune questioni specifiche relative al trattamento, tra cui il software da utilizzare, le modalità di distribuzione dell'accesso all'interno dell'organizzazione ecc. Ciò non altera il suo ruolo di responsabile del trattamento, a condizione che si limiti a trattare i dati in base alle istruzioni impartite dalla società A.

Esempio: pagamenti bancari

Nell'ambito delle istruzioni del datore di lavoro A, l'ufficio stipendi trasmette informazioni alla banca B affinché possa effettuare i pagamenti ai dipendenti del datore di lavoro A. Tale attività prevede il trattamento di dati personali da parte della banca B, che essa svolge ai fini dell'esercizio dell'attività bancaria. Nell'ambito di detta attività, la banca decide indipendentemente dal datore di lavoro A quali dati trattare per erogare il servizio, per quanto tempo i dati devono essere archiviati ecc. Il datore di lavoro A non può influire sulla finalità e sui mezzi del trattamento dei dati da parte della banca B. La banca B va pertanto considerata come titolare ai fini del trattamento e la trasmissione dei dati personali da parte dell'ufficio stipendi va considerata come una comunicazione di informazioni tra due titolari del trattamento, dal datore di lavoro A alla banca B.

Esempio: commercialisti

Il datore di lavoro A si rivolge inoltre alla società contabile C per la revisione della propria contabilità e pertanto trasferisce i dati relativi alle operazioni finanziarie (compresi i dati personali) a detta società contabile C. Quest'ultima tratta tali dati senza istruzioni dettagliate da parte di A: decide autonomamente, conformemente alle disposizioni di legge disciplinanti i compiti delle attività di revisione che svolge in quanto studio contabile, che i dati raccolti saranno trattati unicamente ai fini della revisione contabile di A e determina i dati di cui ha bisogno, quali categorie di persone registrare, per quanto tempo i dati sono archiviati e i mezzi tecnici da impiegare. In siffatte circostanze, la società contabile C va considerata come titolare del trattamento nell'esecuzione dei servizi di revisione contabile per A.

Tuttavia, tale valutazione può differire in base al livello di istruzioni impartite da A. Ove la legge non preveda obblighi specifici per la società contabile e la società cliente fornisca istruzioni molto dettagliate sul trattamento, la società contabile agirebbe di fatto come responsabile del trattamento. Si potrebbe anche distinguere tra una situazione in cui il trattamento è, conformemente alle norme disciplinanti tale professione, effettuato nell'ambito dell'attività principale della società contabile e una diversa situazione in cui il trattamento è un compito accessorio più limitato svolto nell'ambito dell'attività della società cliente.

Esempio: servizi di hosting

Il datore di lavoro A ricorre al servizio di hosting H per archiviare dati criptati sui server di H. Il servizio di hosting H non stabilisce se i dati che ospita sono dati personali né tratta i dati in modo diverso dall'archiviazione nei propri server. Poiché l'archiviazione è un esempio di attività di trattamento di dati personali, il servizio di hosting H tratta dati personali per conto del datore di lavoro A ed è pertanto responsabile del trattamento. Il datore di lavoro A deve impartire le istruzioni necessarie a H e, a norma dell'articolo 28, deve essere concluso un accordo per il trattamento dei dati, con l'obbligo per H di attuare misure tecniche e organizzative di sicurezza. H deve assistere A nel garantire che siano adottate le misure di sicurezza necessarie e notificare ad A i casi di violazione dei dati personali.

41. Anche se le decisioni sui mezzi non essenziali possono essere lasciate al responsabile del trattamento, il titolare del trattamento deve comunque stabilire determinati elementi nell'accordo sul trattamento dei dati quali, ad esempio, in relazione al requisito della sicurezza, l'istruzione di adottare tutte le misure richieste a norma dell'articolo 32 del GDPR. L'accordo deve inoltre prevedere che il responsabile del trattamento assista il titolare nel garantire, ad esempio, l'adempimento degli obblighi di cui all'articolo 32. In ogni caso, il titolare del trattamento rimane responsabile dell'attuazione di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento (articolo 24). Nel far ciò, il titolare del trattamento deve tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e per le libertà delle persone fisiche. Per tale motivo, il titolare del trattamento deve essere pienamente informato dei mezzi utilizzati, in modo da poter adottare una decisione in merito con cognizione di causa. Affinché il titolare del trattamento possa dimostrare la liceità dello stesso è consigliabile documentare quanto meno le misure tecniche e organizzative necessarie nel contratto o in un altro strumento giuridicamente vincolante tra il titolare e il responsabile del trattamento.

Esempio: call center

La società X decide di esternalizzare una parte del servizio clienti a un call center, che quindi riceve dati identificabili sugli acquisti dei clienti nonché informazioni di contatto. Il call center utilizza il proprio software e la propria infrastruttura informatica per gestire i dati personali relativi ai clienti della società X. La società X firma un accordo di trattamento con il fornitore dei servizi di call center, a norma dell'articolo 28 del GDPR, dopo aver stabilito che le misure di sicurezza tecniche e organizzative proposte dal call center stesso sono adeguate ai rischi in questione e che i dati personali saranno trattati unicamente per le finalità della società X e conformemente alle istruzioni della stessa. La società X non impartisce ulteriori istruzioni al call center in merito al software specifico da utilizzare né istruzioni dettagliate sulle misure di sicurezza specifiche da mettere in atto. In questo esempio, la società X rimane titolare del trattamento, nonostante il call center abbia definito determinati mezzi non essenziali del trattamento in questione.

2.1.5 «DEL TRATTAMENTO DEI DATI PERSONALI»

42. Le finalità e i mezzi determinati dal titolare devono riguardare il «trattamento dei dati personali». L'articolo 4, paragrafo 2, del GDPR definisce il trattamento dei dati personali come «qualsiasi operazione o insieme di operazioni [...] applicate a dati personali o insiemi di dati personali». Di conseguenza, il concetto di titolare del trattamento può essere collegato a una singola operazione di trattamento o a una serie di operazioni. In pratica, ciò può significare che il controllo esercitato da un determinato soggetto può estendersi alla totalità del trattamento in questione, ma può anche essere limitato a una fase specifica dello stesso.[16]

43. In pratica, un trattamento di dati personali che coinvolge più soggetti può essere suddiviso in più operazioni di trattamento per ciascuna delle quali ognuno di tali soggetti potrebbe essere considerato titolare, ossia colui che determina la finalità e i mezzi nel singolo caso. D'altro canto, una sequenza o un insieme di trattamenti che coinvolgono più soggetti possono avere luogo anche per la/le medesima/e finalità; in tal caso è possibile che il trattamento coinvolga uno o più contitolari . In altre parole, è possibile che a «livello micro» le diverse operazioni di trattamento della catena appaiano scollegate, in quanto ciascuna di esse può avere una finalità diversa. Tuttavia, è necessario un doppio controllo atto a verificare se, a «livello macro», queste operazioni di trattamento non debbano essere considerate come un «insieme di operazioni» che perseguono una finalità comune mediante mezzi definiti congiuntamente.

44. Chiunque decida di trattare dati deve valutare se questi comprendano dati personali e, in caso affermativo, quali siano gli obblighi previsti dal GDPR. Un soggetto sarà considerato «titolare del trattamento» anche se non tratta deli-

beratamente dati personali in quanto tali o se ha ritenuto, erroneamente, di non trattare dati personali.

45. Non è necessario che il titolare abbia effettivamente accesso ai dati oggetto del trattamento[17]. Un soggetto che esternalizzi un'attività di trattamento e in tal modo eserciti un'influenza determinante sulla finalità e sui mezzi (essenziali) del trattamento stesso (ad esempio configurando i parametri di un servizio in modo tale da definire quali dati personali debbano essere trattati) è da ritenersi il titolare del trattamento anche se non avrà mai accesso effettivo ai dati.

Esempio: ricerche di mercato 1

La società ABC desidera sapere quali tipi di consumatori sono maggiormente interessati ai suoi prodotti e stipula un contratto con il fornitore di servizi XYZ per ottenere informazioni pertinenti.

ABC informa XYZ in merito alle tipologie di informazioni che la interessano e fornisce un elenco di domande da porre ai partecipanti alla ricerca di mercato.

ABC riceve da XYZ solo informazioni statistiche (ad esempio, l'identificazione delle tendenze dei consumatori per regione) e non ha accesso ai dati personali. Tuttavia, la società ABC ha deciso che il trattamento doveva aver luogo, il trattamento è effettuato per le sue finalità e attività e la società ABC ha fornito a XYZ istruzioni dettagliate sulle informazioni da raccogliere. ABC va pertanto ancora considerata titolare del trattamento dei dati personali che ha luogo al fine di fornire le informazioni richieste. XYZ può trattare i dati solo per la finalità indicata dalla società ABC e secondo le sue istruzioni dettagliate e va pertanto considerata come responsabile del trattamento.

Esempio: ricerche di mercato 2

La società ABC desidera sapere quali tipi di consumatori sono maggiormente interessati ai suoi prodotti. Il fornitore di servizi XYZ è un'agenzia di ricerche di mercato che ha raccolto informazioni sugli interessi dei consumatori attraverso una serie di questionari relativi a un'ampia gamma di prodotti e servizi. XYZ ha raccolto e analizzato tali dati in modo indipendente, secondo la propria metodologia, senza ricevere istruzioni dalla società ABC. Per rispondere alla richiesta della società ABC, il fornitore di servizi XYZ genera informazioni statistiche, senza tuttavia ricevere ulteriori istruzioni su quali dati personali vadano trattati o su come trattarli al fine di generare tali statistiche. In questo esempio, il fornitore di servizi XYZ agisce in qualità di titolare unico del trattamento, trattando i dati personali ai fini della ricerca di mercato e determinando autonomamente i mezzi per attuarla. Ai sensi della normativa in materia di prote-

zione dei dati la società ABC non ha alcun ruolo o responsabilità particolari in relazione a tali attività di trattamento, in quanto riceve statistiche anonimizzate e non è coinvolta nella determinazione delle finalità e dei mezzi del trattamento.

3. DEFINIZIONE DI CONTITOLARI DEL TRATTAMENTO

3.1 DEFINIZIONE DI CONTITOLARI DEL TRATTAMENTO

46. La contitolarità di trattamento può configurarsi laddove più di un soggetto sia coinvolto nel trattamento.

47. Sebbene il concetto non sia nuovo e già esistesse ai sensi della direttiva 95/46/CE, il GDPR introduce all'articolo 26 norme specifiche per i contitolari del trattamento e stabilisce un quadro per disciplinarne le relazioni. Inoltre, in sentenze recenti la Corte di giustizia dell'Unione europea (CGUE) ha apportato chiarimenti su questo concetto e sulle sue implicazioni[18].

48. Come ulteriormente precisato nella parte II, sezione 2, la qualifica di contitolari del trattamento avrà principalmente conseguenze in termini di ripartizione degli obblighi di rispetto delle norme in materia di protezione dei dati e, in particolare, per quanto concerne i diritti delle persone fisiche.

49. In tale prospettiva, la sezione seguente mira a fornire orientamenti sul concetto di contitolari del trattamento, ai sensi del GDPR e della giurisprudenza della Corte di giustizia dell'Unione europea, al fine di contribuire alla definizione dei casi ove si sia in presenza di contitolarità nonché all'applicazione concreta di tale nozione.

3.2 ESISTENZA DI UNA CONTITOLARITÀ DEL TRATTAMENTO

3.2.1 CONSIDERAZIONI GENERALI

50. La definizione di titolare del trattamento di cui all'articolo 4, paragrafo 7, del GDPR costituisce il punto di partenza per determinare la contitolarità del trattamento. Le considerazioni di cui alla presente sezione sono pertanto direttamente collegate a quelle di cui alla sezione sul concetto di titolare del trattamento e le integrano. Di conseguenza, la valutazione della contitolarità del trattamento dovrebbe essere speculare a quella concernente la titolarità «unica» di cui sopra.

51. L'articolo 26 del GDPR, che rispecchia la definizione di cui all'articolo 4, paragrafo 7, dello stesso regolamento, stabilisce che «*allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento*.» In termini generali, sussiste una contitolarità del trattamento in relazione a una specifica attività di trattamento

quando soggetti diversi determinano *congiuntamente* la finalità e i mezzi di tale attività di trattamento. Pertanto, per valutare l'esistenza di contitolari del trattamento è necessario esaminare se la determinazione delle finalità e dei mezzi che è prerogativa del titolare del trattamento sia appannaggio di più di un solo soggetto. Il termine «congiuntamente» deve essere interpretato nel senso di «insieme con» o «non isolatamente», in diverse forme e combinazioni, come spiegato nel prosieguo.

52. La valutazione della contitolarità del trattamento dovrebbe essere fondarsi su di un'analisi fattuale, piuttosto che formale, dell'influenza effettivamente esercitata sulle finalità e sui mezzi del trattamento. Qualsivoglia configurazione esistente o prevista dovrebbe essere verificata alla luce delle circostanze concretamente relative al rapporto tra le parti. Un criterio meramente formale non sarebbe sufficiente per almeno due motivi: in taluni casi, la designazione formale di un contitolare del trattamento, prevista ad esempio ai sensi di legge o da un contratto, potrebbe mancare; in altri casi, può risultare che la designazione formale non rispecchi la realtà dei meccanismi in atto, poiché si attribuisce formalmente il ruolo di titolare del trattamento a un soggetto che di fatto non è in grado di «determinare» le finalità e i mezzi del trattamento.

53. Non tutti i trattamenti che coinvolgono più soggetti danno luogo a una contitolarità del trattamento. Il criterio generale per la sussistenza della contitolarità del trattamento è la **partecipazione congiunta di due o più soggetti alla determinazione delle finalità e dei mezzi** dello stesso. Più specificamente, la partecipazione congiunta deve comprendere, da un lato, la determinazione delle finalità e, dall'altro, la determinazione dei mezzi. Se ciascuno di questi elementi è determinato da tutti i soggetti coinvolti, questi ultimi dovrebbero essere considerati contitolari del trattamento in questione.

3.2.2 VALUTAZIONE DELLA PARTECIPAZIONE CONGIUNTA

54. La partecipazione congiunta nella determinazione delle finalità e dei mezzi implica che più soggetti esercitino un'influenza determinante sull'effettuazione del trattamento e sulle relative modalità. In pratica, la partecipazione congiunta può assumere diverse forme, come, ad esempio, quella di una **decisione comune** presa da due o più soggetti, oppure derivare da **decisioni convergenti** di due o più soggetti per quanto concerne le finalità e i mezzi essenziali.

55. La partecipazione congiunta mediante una *decisione comune* implica l'assunzione di una decisione e un'intenzione condivisa di adottare tale decisione, in base all'interpretazione più corrente del termine «congiuntamente» di cui all'articolo 26 del GDPR.

    La situazione della partecipazione congiunta attraverso decisioni convergenti deriva in particolare dalla giurisprudenza della CGUE sul concetto di contitolari del trattamento. Le decisioni possono essere considerate convergenti sulle finalità e sui mezzi **se si integrano a vicenda e se sono necessarie affinché il trattamento abbia luogo, in modo tale da avere un impatto**

tangibile sulla determinazione delle finalità e dei mezzi del trattamento. Occorre sottolineare che il concetto di decisioni convergenti va considerato in relazione alle finalità e ai mezzi del trattamento, ma non con riguardo ad altri aspetti del rapporto commerciale tra le parti[19]. In tal senso, un criterio importante per individuare decisioni convergenti in questo ambito **consiste nel verificare se il trattamento non sarebbe possibile senza la partecipazione di entrambe le parti alle finalità e ai mezzi, nel senso che i trattamenti di ciascuna parte sono tra loro indissociabili, ovverosia indissolubilmente legati**. La situazione in cui contitolari del trattamento agiscono sulla base di decisioni convergenti dovrebbe tuttavia essere distinta da quella del responsabile del trattamento, poiché quest'ultimo, pur partecipando all'esecuzione dello stesso, non tratta i dati per le proprie finalità ma per conto del relativo titolare.

56. Il fatto che una delle parti non abbia accesso ai dati personali trattati non è sufficiente per escludere la contitolarità del trattamento[20]. Ad esempio, nella causa *Testimoni di Geova* la CGUE ha ritenuto che una comunità religiosa dovesse essere considerata titolare, insieme ai suoi membri praticanti la predicazione, del trattamento dei dati personali effettuato da questi ultimi nell'ambito della predicazione porta a porta[21]. La CGUE ha ritenuto che non fosse necessario che la comunità avesse accesso ai dati in questione né stabilire che avesse fornito ai suoi membri linee guida o istruzioni scritte in relazione al trattamento di dati[22]. La comunità ha partecipato alla determinazione delle finalità e dei mezzi organizzando e coordinando le attività dei propri membri, il che ha contribuito al perseguimento dell'obiettivo della stessa comunità dei Testimoni di Geova[23]. Inoltre, la comunità era a conoscenza, a livello generale, del fatto che tale trattamento veniva effettuato al fine di diffondere il proprio credo[24].

57. È altresì importante sottolineare, come chiarito dalla CGUE, che un soggetto sarà considerato contitolare del trattamento insieme ad altri solo per quelle operazioni rispetto alle quali determina, insieme ad altri, i mezzi e le finalità di quello stesso trattamento dei dati, in particolare in caso di decisioni convergenti. Se uno dei soggetti in questione decide isolatamente le finalità e i mezzi delle operazioni precedenti o successive nelle varie fasi del trattamento, tale soggetto deve essere considerato l'unico titolare di tale operazione di trattamento precedente o successiva[25].

58. L'esistenza di una responsabilità congiunta non implica necessariamente pari responsabilità dei vari operatori coinvolti nel trattamento dei dati personali. Al contrario, la CGUE ha chiarito che tali operatori possono essere coinvolti in fasi diverse di tale trattamento e in misura diversa, cosicché il livello di responsabilità di ciascuno di essi deve essere valutato alla luce di tutte le circostanze pertinenti del caso di specie.

3.2.2.1 Determinazione congiunta delle finalità

59. Una contitolarità del trattamento sussiste allorquando soggetti coinvolti nel medesimo trattamento lo effettuano per finalità definite congiuntamente. Ciò avviene se i soggetti in questione trattano i dati per le medesime finalità o per finalità comuni.

60. Inoltre, laddove tali soggetti non perseguano la medesima finalità in relazione al trattamento, alla luce della giurisprudenza della Corte di giustizia dell'Unione europea la contitolarità del trattamento può configurarsi anche qualora i soggetti perseguano finalità strettamente collegate o complementari. Ciò può verificarsi, ad esempio, quando esiste un vantaggio reciproco derivante dalla medesima operazione di trattamento, a condizione che ciascuno dei soggetti coinvolti partecipi alla determinazione delle finalità e dei mezzi del trattamento in questione. Tuttavia, il concetto di vantaggio reciproco non è decisivo e ha valore puramente indicativo. In *Fashion ID*, ad esempio, la CGUE ha chiarito che un gestore di siti web partecipa alla determinazione delle finalità (e dei mezzi) del trattamento inserendo un «plug-in social» su un sito web, al fine di ottimizzare la pubblicità dei propri prodotti rendendoli più visibili sul social network. La CGUE ha ritenuto che le operazioni di trattamento in questione fossero effettuate nell'interesse economico sia dell'operatore del sito internet che del fornitore del plug-in social[26].

61. Analogamente, come rilevato dalla CGUE nella causa *Wirtschaftsakademie*, il trattamento di dati personali mediante statistiche dei visitatori di una «fanpage» mira a consentire a Facebook di migliorare il sistema di pubblicità trasmessa attraverso la propria rete e consente al gestore della fanpage di ottenere statistiche per gestire la promozione della propria attività[27]. In tal caso ogni soggetto persegue il proprio interesse, ma per quanto concerne i visitatori della fanpage entrambi partecipano alla determinazione delle finalità (e dei mezzi) del trattamento dei dati personali[28].

62. A tale riguardo, è importante sottolineare che la semplice esistenza di un vantaggio reciproco (ad esempio di natura commerciale), derivante da un'attività di trattamento, non comporta una contitolarità del trattamento. Se il soggetto coinvolto nel trattamento non persegue alcuna finalità propria in relazione allo stesso, ma viene semplicemente remunerato per i servizi prestati, esso agisce in qualità di responsabile del trattamento anziché di contitolare.

3.2.2.2 Determinazione congiunta dei mezzi

63. La contitolarità del trattamento prevede, inoltre, che due o più soggetti abbiano esercitato un'influenza sui mezzi del trattamento. Ciò non significa che, affinché sussista una contitolarità del trattamento, ciascun soggetto coinvolto debba in ogni caso determinarne tutti i mezzi. Di fatto, come chiarito dalla CGUE, soggetti diversi possono essere coinvolti in fasi diverse del trattamento e a livelli diversi. I diversi contitolari del trattamento possono pertanto determinare i mezzi del trattamento in misura diversa, a seconda di chi sia effettivamente in grado di effettuare tale determinazione.

64. Può anche accadere che uno dei soggetti coinvolti fornisca i mezzi del trattamento e li metta a disposizione per le attività di trattamento dei dati personali da parte di altri soggetti. Anche il soggetto che decide di avvalersi di tali mezzi affinché i dati personali possano essere trattati per una determinata finalità partecipa alla determinazione dei mezzi del trattamento.

65. Tale situazione può verificarsi, in particolare, nel caso di piattaforme, strumenti standardizzati o di altre infrastrutture che consentono alle parti di trattare gli stessi dati personali e che sono stati predisposti in un certo modo da una delle parti per essere utilizzati da altre che possono anche decidere come impostarli[29]. L'uso di un sistema tecnico già esistente non esclude la contitolarità del trattamento laddove gli utenti del sistema possano decidere in merito al trattamento dei dati personali da effettuare in tale contesto.

66. A titolo di esempio, nella sentenza *Wirtschaftsakademie* la CGUE ha statuito che, nel definire i parametri basati sul pubblico destinatario e sugli obiettivi di gestione e promozione delle proprie attività, l'amministratore di una «fanpage» su Facebook dovesse essere considerato come un soggetto che partecipa alla determinazione dei mezzi di trattamento dei dati personali dei relativi visitatori.

67. Inoltre, la scelta da parte di un soggetto di utilizzare per le proprie finalità uno strumento o un altro sistema sviluppato da altri per il trattamento di dati personali costituirà probabilmente una decisione congiunta sui mezzi di tale trattamento da parte dei soggetti in questione. Ciò risulta dalla causa *Fashion ID*, in cui la CGUE ha concluso che, inserendo nel proprio sito internet il pulsante Facebook Like, messo da Facebook a disposizione degli operatori di siti web, *Fashion ID* ha esercitato un'influenza determinante sulle operazioni che comportano la raccolta e la trasmissione dei dati personali dei visitatori del suo sito internet a Facebook e ha pertanto determinato, congiuntamente con Facebook, i mezzi di tale trattamento[30].

68. È importante sottolineare che **l'uso di un sistema o di un'infrastruttura comuni per il trattamento dei dati non comporterà in tutti i casi la contitolarità del trattamento da parte dei soggetti coinvolti**, in particolare allorquando il trattamento da essi effettuato è scindibile e potrebbe essere eseguito da un soggetto senza l'intervento dell'altro, o se il fornitore è un responsabile del trattamento che non persegue una finalità propria (l'esistenza di un mero vantaggio commerciale per le parti coinvolte non è sufficiente a configurare una finalità di trattamento).

Esempio: agenzia di viaggi

Un'agenzia di viaggi invia alla compagnia aerea e a una catena di alberghi i dati personali dei propri clienti, al fine di effettuare prenotazioni per un pacchetto turistico. La compagnia aerea e l'albergo confermano la disponibilità dei posti e delle camere richiesti. L'agenzia di viaggi rilascia ai clienti i documenti di viaggio e i buoni. Ciascuno dei soggetti tratta i dati per svolgere le proprie attività e utilizzando i propri mezzi. In questo caso, l'agenzia di viaggi, la compagnia aerea e l'albergo sono tre distinti titolari del trattamento che perseguono finalità autonome e separate e non sussiste una contitolarità del trattamento.

L'agenzia di viaggi, la catena alberghiera e la compagnia aerea decidono poi di partecipare congiuntamente alla creazione di una piattaforma comune su internet per la finalità comune di offrire pacchetti turistici.

Concordano i mezzi essenziali da utilizzare, quali i dati da archiviare, le modalità di assegnazione e conferma delle prenotazioni e chi può avere accesso alle informazioni memorizzate. Inoltre, decidono di condividere i dati dei clienti al fine di effettuare operazioni di marketing congiunte. In questo caso, l'agenzia di viaggi, la compagnia aerea e la catena alberghiera determinano congiuntamente le finalità e le modalità di trattamento dei dati personali dei rispettivi clienti e saranno pertanto contitolari del trattamento per quanto riguarda le operazioni di trattamento relative alla piattaforma comune di prenotazione via internet e le operazioni congiunte di marketing. Tuttavia, ciascuna di esse manterrebbe la titolarità esclusiva di altre attività di trattamento svolte al di fuori della piattaforma comune su internet.

Esempio: progetto di ricerca da parte di più istituti

Diversi istituti di ricerca decidono di partecipare a un progetto comune specifico e di utilizzare a tal fine la piattaforma esistente di uno di essi. Ai fini della ricerca congiunta ciascun istituto alimenta la piattaforma con i dati personali che detiene e utilizza i dati forniti da altri attraverso la piattaforma per svolgere l'attività di ricerca. In questo caso, tutti gli istituti si qualificano come contitolari del trattamento dei dati personali svolto mediante l'archiviazione e la divulgazione di informazioni provenienti dalla piattaforma, in quanto hanno deciso congiuntamente la finalità del trattamento e i mezzi da utilizzare (la piattaforma esistente). Tuttavia, ciascuno degli istituti è un titolare autonomo rispetto a qualsivoglia trattamento effettuato al di fuori della piattaforma per proprie finalità.

Esempio: operazione di marketing

Le società A e B hanno lanciato un prodotto con il marchio comune C e desiderano organizzare un evento per promuovere tale prodotto. A tal fine decidono di condividere dati tratti dai rispettivi database della clientela esistente e potenziale e su tale base decidono in merito all'elenco degli invitati all'evento. Concordano inoltre le modalità di invio degli inviti all'evento, le modalità di raccolta dei riscontri durante lo stesso e il follow-up delle operazioni di marketing. Le società A e B possono essere considerate contitolari del trattamento dei dati personali relativo all'organizzazione dell'evento promozionale in quanto decidono congiuntamente, in tale contesto, in merito alla determinazione congiunta della finalità e dei mezzi essenziali del trattamento.

Esempio: sperimentazioni cliniche[31]

Un prestatore di assistenza sanitaria (lo sperimentatore) e un'università (lo sponsor) decidono di avviare congiuntamente una sperimentazione

clinica avente la medesima finalità. Collaborano all'elaborazione del protocollo di studio (ossia finalità, metodologia/progettazione dello studio, dati da raccogliere, criteri di esclusione/inclusione dei soggetti, riutilizzo delle banche dati, se del caso, ecc.). Possono essere considerati contitolari del trattamento per detta sperimentazione clinica in quanto stabiliscono e concordano congiuntamente una stessa finalità e i mezzi essenziali del trattamento. La raccolta di dati personali dalla cartella clinica del paziente ai fini di ricerca va distinta dalla conservazione e dall'uso degli stessi dati ai fini dell'assistenza del paziente, per i quali il fornitore di assistenza sanitaria rimane titolare del trattamento.

Nel caso in cui lo sperimentatore non partecipi alla stesura del protocollo (in quanto accetta semplicemente il protocollo già elaborato dallo sponsor) e il protocollo sia elaborato solo dallo sponsor, ai fini della sperimentazione clinica il ricercatore dovrebbe essere considerato responsabile del trattamento e lo sponsor il titolare del trattamento.

Esempio: agenzie di selezione di personale («*headhunters*»)

La società X aiuta la società Y ad assumere nuovo personale mediante il suo famoso servizio a valore aggiunto «global matchz». La società X cerca candidati idonei sia tra i CV ricevuti direttamente dalla società Y che tra quelli già presenti nella propria banca dati. Tale banca dati è creata e gestita dalla sola società X. Così facendo la società X può migliorare la corrispondenza tra offerte e richieste di lavoro, incrementando le entrate. Sebbene non abbiano formalmente assunto una decisione congiunta, le società X e Y partecipano congiuntamente al trattamento, al fine di individuare candidati idonei sulla base di decisioni convergenti: la decisione di creare e di gestire il servizio «global matchz» per la società X, e la decisione della società Y di arricchire la banca dati con i CV che riceve direttamente. Tali decisioni si integrano reciprocamente, sono indissociabili e necessarie per il trattamento connesso alla ricerca di candidati idonei. Pertanto, in questo caso particolare, X e Y dovrebbero essere considerate contitolari di tale trattamento. Tuttavia, la società X è l'unico titolare del trattamento necessario per la gestione della propria banca dati e la società Y è l'unico titolare del successivo trattamento di assunzione per le proprie finalità (organizzazione dei colloqui, conclusione del contratto e gestione dei dati delle risorse umane).

Esempio: analisi dei dati sanitari

La società ABC, che ha sviluppato un'applicazione per il monitoraggio della pressione sanguigna, e la società XYZ, fornitore di applicazioni per professionisti del settore medico, desiderano esaminare in che modo le variazioni della pressione sanguigna possano contribuire a prevedere determinate malattie. Le società decidono di avviare un progetto comune e di coinvolgere anche l'ospedale DEF.

I dati personali che saranno trattati nell'ambito del progetto sono quelli che la società ABC, l'ospedale DEF e la società XYZ trattano separatamente in quanto titolari autonomi di trattamento. La decisione di trattare i dati per valutare le variazioni di pressione sanguigna è presa congiuntamente dai tre soggetti. La società ABC, l'ospedale DEF e la società XYZ hanno stabilito congiuntamente le finalità del trattamento. La società XYZ prende l'iniziativa di proporre i mezzi essenziali del trattamento. Sia la società ABC che l'ospedale DEF approvano detti mezzi essenziali dopo essere stati anch'essi coinvolti nello sviluppo di alcune caratteristiche dell'applicazione, in modo tale da poterne utilizzare i risultati in misura sufficiente. I tre soggetti convengono quindi di perseguire una finalità comune per il trattamento, ossia valutare in che modo le variazioni della pressione sanguigna possano contribuire alla previsione di determinate malattie. Una volta completata la ricerca, la società ABC, l'ospedale DEF e la società XYZ potranno beneficiare della valutazione utilizzando i risultati nell'ambito delle rispettive attività. Per tutti questi motivi, essi si qualificano come contitolari di tale specifico trattamento congiunto.

Se la società XYZ fosse stata semplicemente invitata dalle altre a effettuare tale valutazione senza avere alcuna finalità propria e trattando i dati per conto delle altre, essa si qualificherebbe come responsabile del trattamento anche qualora fosse stata incaricata della determinazione dei mezzi non essenziali di tale trattamento.

3.2.3 SITUAZIONI IN CUI NON SUSSISTE CONTITOLARITÀ DEL TRATTAMENTO

69. Il fatto che più soggetti siano coinvolti nello stesso trattamento non significa che essi agiscano necessariamente in qualità di contitolari del trattamento. Non tutti i tipi di partenariato, cooperazione o collaborazione implicano la qualifica di contitolari del trattamento, in quanto è necessaria un'analisi caso per caso di ciascun trattamento in questione e del ruolo preciso svolto da ciascun soggetto in relazione a tale trattamento. I casi che seguono forniscono esempi non esaustivi di situazioni in cui non sussiste contitolarità del trattamento.

70. Ad esempio, lo scambio degli stessi dati o insiemi di dati tra due soggetti in assenza di finalità o mezzi di trattamento determinati congiuntamente dovrebbe essere considerato una trasmissione di dati tra titolari del trattamento distinti.

Esempio: trasmissione dei dati dei dipendenti alle autorità fiscali

Una società raccoglie e tratta i dati personali dei propri dipendenti allo scopo di gestire le retribuzioni, le assicurazioni malattia ecc. La legge impone alla società l'obbligo di inviare alle autorità fiscali tutti i dati relativi alle retribuzioni, al fine di un controllo fiscale più accurato.

In questo caso, anche se tanto la società quanto le autorità fiscali trattano

gli stessi dati relativi alle retribuzioni, la mancanza di una determinazione congiunta della finalità e dei mezzi riferiti a tale trattamento dei dati porterà a qualificare i due soggetti come titolari distinti del trattamento dei dati.

71. La contitolarità del trattamento può essere esclusa anche nel caso in cui più soggetti utilizzino una banca dati condivisa o un'infrastruttura comune, qualora ciascuna di esse determini autonomamente le proprie finalità.

Esempio: operazioni commerciali all'interno di un gruppo societario che utilizza una banca dati condivisa

Un gruppo di società utilizza la stessa banca dati per la gestione dei clienti (esistenti e potenziali). La banca dati è ospitata sui server della società controllante, che agisce pertanto da responsabile del trattamento delle controllate per quanto riguarda l'archiviazione dei dati. Ciascun soggetto appartenente al gruppo inserisce i dati dei propri clienti (esistenti e potenziali) e li elabora esclusivamente per le proprie finalità. Inoltre, ciascun soggetto decide autonomamente in merito all'accesso, ai periodi di archiviazione, alla rettifica o alla cancellazione dei dati dei propri clienti e potenziali tali, senza potere accedere ai dati degli altri partecipanti o utilizzarli. Il semplice fatto che tali società utilizzino una banca dati condivisa non comporta, di per sé, una contitolarità del trattamento. In siffatte circostanze, ciascuna società è pertanto un titolare del trattamento distinto.

Esempio: titolari indipendenti che utilizzano un'infrastruttura condivisa

La società XYZ ospita una banca dati e la mette a disposizione di altre società per il trattamento e l'archiviazione dei dati personali relativi ai dipendenti di tali altre società. La società XYZ è un responsabile del trattamento in quanto tratta e archivia i dati dei dipendenti di altre società per conto e secondo le istruzioni di queste ultime. Inoltre, le altre società trattano i dati senza alcuna partecipazione da parte della società XYZ e per finalità che non sono in alcun modo condivise da quest'ultima.

72. Vi possono essere altresì situazioni in cui vari soggetti trattano successivamente gli stessi dati personali in una catena di operazioni: ciascuno di essi ha una finalità indipendente e impiega mezzi indipendenti relativamente al segmento della catena di rispettiva competenza. In mancanza di una partecipazione congiunta nella determinazione delle finalità e dei mezzi di una stessa operazione di trattamento o dello stesso insieme di operazioni di trattamento, la contitolarità deve essere esclusa e i vari soggetti devono essere considerati come titolari del trattamento indipendenti che agiscono in momenti successivi.

Esempio: analisi statistica per un compito di interesse pubblico

Un'autorità pubblica (autorità A) ha il compito stabilito per legge di elaborare analisi e statistiche sull'evoluzione del tasso di occupazione nel paese. A tal fine, numerosi altri soggetti pubblici sono tenuti per legge a comunicare dati specifici all'autorità A, che decide di utilizzare un sistema specifico per trattare i dati, ivi compresa la raccolta. Ciò significa fra l'altro che le altre autorità pubbliche sono obbligate a utilizzare tale sistema per la comunicazione dei dati. In questo caso, fatta salva l'eventuale attribuzione dei ruoli per legge, l'autorità A sarà l'unico titolare del trattamento ai fini dell'analisi e delle statistiche del tasso di occupazione attraverso il sistema, in quanto determina la finalità del trattamento e ha deciso in merito alla modalità di organizzazione dello stesso. Naturalmente, gli altri soggetti pubblici, in quanto titolari delle rispettive attività di trattamento, hanno la responsabilità di garantire l'esattezza dei dati da essi precedentemente trattati e successivamente comunicati all'autorità A.

4. DEFINIZIONE DI RESPONSABILE DEL TRATTAMENTO

73. L'articolo 4, paragrafo 8, definisce il responsabile del trattamento come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Analogamente alla definizione di titolare del trattamento, la definizione di responsabile del trattamento prevede un'ampia gamma di soggetti: può trattarsi di *una persona fisica o giuridica, un'autorità pubblica, un servizio o un altro organismo.* Ciò significa che, in linea di principio, non vi sono limitazioni riguardo alle caratteristiche soggettive del responsabile del trattamento. Potrebbe trattarsi di un'organizzazione, ma anche di un singolo.

74. Il GDPR stabilisce obblighi direttamente e specificamente applicabili ai responsabili del trattamento, come meglio illustrato nella parte II, sezione 1, delle presenti linee guida. Il responsabile del trattamento può essere ritenuto responsabile o sanzionato in caso di inadempimento di detti obblighi o qualora agisca al di fuori o in contrasto con le istruzioni legittime del titolare del trattamento.

75. Il trattamento dei dati personali può coinvolgere più responsabili. Ad esempio, un titolare del trattamento può decidere di utilizzare direttamente più responsabili del trattamento, coinvolgendone diversi in fasi separate dello stesso (molteplici responsabili del trattamento). Un titolare del trattamento potrebbe anche decidere di rivolgersi a un solo responsabile del trattamento che, a sua volta, previa autorizzazione dello stesso titolare, utilizza uno o più responsabili del trattamento («sub-responsabili»). L'attività affidata al responsabile del trattamento può essere limitata a un compito o a un contesto molto specifico o può essere di natura più generale e ampia.

76. Le due condizioni fondamentali per la qualifica di responsabile del trattamento sono:

- essere un *soggetto distinto* rispetto al titolare del trattamento;
- trattare i dati personali *per conto del titolare del trattamento*.

77. *Un soggetto distinto* significa che il titolare del trattamento decide di delegare tutte o parte delle attività di trattamento a un soggetto esterno. All'interno di un gruppo di società, una di esse può essere responsabile del trattamento di un'altra che agisce in qualità di titolare del trattamento, in quanto le due società sono entità distinte. Di converso, un dipartimento all'interno di una società non può essere responsabile del trattamento per conto di un altro dipartimento all'interno della stessa società.

78. Se il titolare del trattamento decide di trattare direttamente i dati utilizzando le proprie risorse interne, ad esempio attraverso il proprio personale, non vi sono responsabili del trattamento. I dipendenti e le altre persone che agiscono sotto l'autorità diretta del titolare del trattamento, come il personale assunto temporaneamente, non vanno considerati responsabili del trattamento poiché trattano dati personali in quanto parte della struttura del titolare del trattamento. Conformemente all'articolo 29, essi sono altresì vincolati dalle istruzioni del suddetto titolare.

79. *Il trattamento di dati personali per conto del titolare* comporta innanzitutto che il soggetto distinto tratti i dati personali a beneficio del titolare del trattamento. All'articolo 4, paragrafo 2, per trattamento si intende un'ampia gamma di operazioni, dalla raccolta alla conservazione, dalla consultazione all'uso, dalla diffusione o qualsiasi altra forma di messa a disposizione fino alla distruzione. Il concetto di «trattamento» è ulteriormente trattato al punto 2.1.5 che precede.

80. In secondo luogo, il trattamento deve essere effettuato per conto di un titolare, ma non agendo sotto la sua autorità o controllo diretti. Agire «per conto di» significa servire gli interessi di terzi e richiama la nozione giuridica di «delega». Nel caso della normativa in materia di protezione dei dati, il responsabile del trattamento è chiamato a seguire le istruzioni impartite dal titolare almeno per quanto concerne la finalità del trattamento e gli elementi essenziali che ne costituiscono i mezzi. La liceità del trattamento, ai sensi dell'articolo 6 e, se pertinente, dell'articolo 9 del regolamento, deriva dall'attività del titolare del trattamento: il responsabile del trattamento non deve trattare i dati in modo diverso da quanto indicato nelle istruzioni del suddetto titolare. Tuttavia, come detto in precedenza, le istruzioni del titolare del trattamento possono lasciare un certo margine di discrezionalità su come servire al meglio i suoi interessi; ciò consente al responsabile del trattamento di scegliere i mezzi tecnici e organizzativi più idonei[32].

81. Agire «per conto di» significa inoltre che il responsabile del trattamento non può effettuare trattamenti per finalità proprie. Ai sensi dell'articolo 28, paragrafo 10, il responsabile del trattamento è in violazione del GDPR qualora non si limiti a trattare i dati in base alle istruzioni del titolare del trattamento e inizi a definire proprie finalità e propri mezzi di trattamento. Il responsabile del trattamento si configura come titolare in un caso del genere e può essere soggetto a sanzioni qualora non si limiti a trattare i dati in base alle istruzioni del titolare.

Esempio: prestatore di servizi indicato come responsabile del trattamento ma che agisce in qualità di titolare del trattamento

Il fornitore di servizi MarketinZ fornisce servizi di pubblicità promozionale e di marketing diretto a varie società. La società GoodProductZ conclude un contratto con MarketinZ, in base al quale quest'ultima fornisce servizi di pubblicità commerciale ai clienti di GoodProductZ ed è designata responsabile del trattamento dei dati. Tuttavia, MarketinZ decide di utilizzare la banca dati dei clienti di GoodProductZ anche per finalità diverse dalla pubblicità per GoodProductZ, ad esempio per sviluppare la propria attività commerciale. La decisione di aggiungere un'ulteriore finalità a quella per la quale i dati personali sono stati trasferiti converte MarketinZ in titolare del trattamento dei dati per questa serie di operazioni di trattamento e il trattamento a tal fine costituirebbe una violazione del GDPR.

82. L'EDPB rammenta che, ai sensi del GDPR, non tutti i fornitori di servizi che trattano dati personali nel corso della prestazione di detti servizi sono «responsabili del trattamento». Il ruolo di responsabile del trattamento non scaturisce dalle caratteristiche del soggetto che tratta dati, ma dalle sue attività concrete in un contesto specifico. In altre parole, uno stesso soggetto può agire contemporaneamente come titolare del trattamento per determinate operazioni di trattamento e come responsabile del trattamento per altre; inoltre la qualifica di titolare o di responsabile del trattamento deve essere valutata in relazione a un insieme specifico di dati o di operazioni. La natura del servizio determinerà se l'attività di trattamento abbia per oggetto il trattamento di dati personali per conto del titolare ai sensi del GDPR. In pratica, se il servizio prestato non è destinato specificamente al trattamento di dati personali o se non prevede tale trattamento come un elemento essenziale, il prestatore del servizio può essere in grado di determinare in modo indipendente le finalità e i mezzi di tale trattamento necessario ai fini della prestazione. In siffatta situazione, il prestatore di servizi va considerato come un autonomo titolare del trattamento e non come responsabile dello stesso[33]. Resta tuttavia necessaria un'analisi caso per caso per stabilire il grado di influenza esercitata da ciascun soggetto nella determinazione delle finalità e dei mezzi del trattamento.

Esempio: servizio di taxi

Un servizio di taxi offre una piattaforma online che consente alle società di prenotare un taxi per trasportare dipendenti o ospiti da e verso l'aeroporto. Al momento della prenotazione di un taxi, la società ABC specifica il nome del dipendente che dovrebbe essere prelevato dall'aeroporto in modo che il conducente possa verificarne l'identità all'arrivo. In questo caso, il servizio taxi tratta i dati personali del dipendente nell'ambito del servizio prestato alla società ABC, ma il trattamento in quanto tale non è l'obiettivo del servizio. Il servizio taxi ha concepito la piattaforma di prenotazione online come

parte dello sviluppo della propria attività commerciale per fornire servizi di trasporto, senza alcuna istruzione da parte della società ABC. Il servizio taxi determina inoltre in modo indipendente le categorie dei dati raccolti e la durata dell'archiviazione. Il servizio agisce quindi in quanto titolare del trattamento pienamente autonomo, malgrado il fatto che il trattamento dei dati abbia luogo a seguito di una richiesta di prestazione del servizio da parte della società ABC.

83. L'EDPB osserva che un fornitore di servizi può comunque agire come responsabile del trattamento anche laddove il trattamento dei dati personali non sia l'oggetto principale o primario del servizio, a condizione che, nella pratica, il cliente del servizio continui a determinarne le finalità e i mezzi. Nel decidere se affidare o meno il trattamento dei dati personali a un determinato prestatore di servizi, i titolari del trattamento dovrebbero valutare attentamente se il prestatore dei servizi in questione consenta loro di esercitare un livello di controllo sufficiente, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi potenziali per gli interessati.

Esempio: call center

La società X esternalizza l'assistenza al cliente alla società Y, che mette a disposizione un call center per agevolare le risposte ai clienti della società X. La fornitura del servizio di assistenza clienti implica che la società Y abbia accesso alle banche dati relative ai clienti della società X. La società Y può accedere ai dati solo per fornire l'assistenza che la società X ha acquistato e non può trattare i dati per finalità diverse da quelle dichiarate dalla società X. La società Y deve essere considerata responsabile del trattamento dei dati personali e tra la società X e la Y deve essere concluso un accordo di trattamento.

Esempio: servizi informatici generali

La società Z si rivolge a un fornitore di servizi informatici per la manutenzione generale dei propri sistemi informatici che contengono una grande quantità di dati personali. L'accesso ai dati personali non è l'oggetto principale del servizio di assistenza, ma è inevitabile che il fornitore di servizi informatici vi abbia sistematicamente accesso durante la fornitura del servizio. La società Z desume pertanto che il fornitore di servizi informatici, essendo una società distinta che inevitabilmente è tenuta a trattare dati personali, anche se questo non è l'obiettivo principale del servizio, debba essere considerata responsabile del trattamento. Un accordo di trattamento è pertanto concluso con il fornitore di servizi informatici.

Esempio: consulente informatico che risolve un problema di software

La società ABC si rivolge a uno specialista informatico di un'altra società per risolvere un «bug» in un proprio software. Il consulente informatico non è ingaggiato per trattare dati personali e la società ABC stabilisce che l'accesso a tali dati sarà puramente accessorio e, pertanto, estremamente limitato nella pratica. La società ABC conclude pertanto che lo specialista informatico non sia responsabile del trattamento (né un autonomo titolare del trattamento) e decide di adottare misure adeguate, a norma dell'articolo 32 del GDPR, al fine di impedirgli di trattare i dati personali in modo non autorizzato.

84. Come indicato in precedenza, nulla osta a che un responsabile del trattamento offra un servizio secondo caratteristiche predeterminate, ma il titolare deve prendere la decisione finale di approvare attivamente le modalità di esecuzione del trattamento, almeno per quanto concerne i mezzi essenziali dello stesso. Come detto, un responsabile del trattamento dispone di un margine di manovra per quanto riguarda i mezzi non essenziali (cfr. la sottosezione 2.1.4).

Esempio: fornitore di servizi cloud

Un comune ha deciso di utilizzare un fornitore di servizi cloud per la gestione delle informazioni nei propri servizi scolastici e di istruzione. Il servizio cloud fornisce servizi di messaggistica, videoconferenze, archiviazione di documenti, gestione del calendario, trattamento testi, ecc. e ciò comporterà il trattamento di dati personali relativi agli alunni e agli insegnanti. Il fornitore di servizi cloud ha proposto un servizio standardizzato, offerto a livello mondiale. Il comune deve comunque assicurarsi che l'accordo in vigore sia conforme all'articolo 28, paragrafo 3, del GDPR, e che i dati personali di cui è titolare siano trattati esclusivamente per le proprie finalità. Deve inoltre assicurarsi che le sue istruzioni specifiche, concernenti per esempio i periodi di archiviazione, la cancellazione dei dati ecc. siano rispettate dal fornitore di servizi cloud, indipendentemente da quanto previsto in via generale dal servizio standardizzato.

5. DEFINIZIONE DI TERZO/DESTINATARIO

85. Il regolamento definisce non solo i concetti di titolare del trattamento e di responsabile del trattamento, ma anche quelli di destinatario e di terzo. A differenza di quanto avviene per il titolare e il responsabile del trattamento, il regolamento non stabilisce obblighi o responsabilità specifici per i destinatari e i terzi. Si tratta di concetti relazionali, nel senso che rimandano a una relazione con un titolare o con un responsabile del trattamento da una prospettiva specifica; ad esempio, il titolare del trattamento o il responsabile del trattamento comunica i dati a un destinatario. Un destinatario di dati personali e un terzo possono essere considerati al contempo titolari o responsabi-

li del trattamento da altri punti di vista. Ad esempio, soggetti da considerarsi destinatari o terzi sotto un determinato punto di vista, sono per altri versi titolari di un trattamento del quale determinano la finalità e i mezzi.

Terzi

86. L'articolo 4, paragrafo 10, definisce «terzo» la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia:

- l'interessato,
- il titolare del trattamento,
- il responsabile del trattamento e
- le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile del trattamento.

87. La definizione corrisponde in linea generale alla precedente definizione di *«terzi»* di cui alla direttiva 95/46/CE.

88. Mentre i termini *«dati personali», «interessato», «titolare del trattamento»* e *«responsabile del trattamento»* sono definiti dal regolamento, non lo è il concetto di *«persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile [del trattamento]»*. Tuttavia, generalmente si intende che con tale formulazione ci si riferisca a persone appartenenti alla struttura giuridica del titolare o del responsabile del trattamento (un dipendente o una persona che occupi una posizione molto simile a quella di dipendente, ad esempio il personale fornito da un'agenzia di lavoro interinale), ma solo nella misura in cui siano autorizzate a trattare dati personali. Non rientra in suddetta categoria un lavoratore dipendente o un'altra figura professionale che acceda a dati ai quali non è autorizzato ad accedere e per finalità diverse da quelle del datore di lavoro. Un tale dipendente dovrebbe invece essere considerato terzo rispetto al trattamento effettuato dal datore di lavoro. Nella misura in cui il dipendente tratti dati personali per le proprie finalità, diverse da quelle del datore di lavoro, sarà considerato titolare del trattamento, risponderà di tutte le conseguenze e si assumerà tutte le responsabilità che ne derivano in termini di trattamento dei dati personali[34].

89. Per "terzo" si intende pertanto un soggetto che, nella specifica situazione in esame, non è né un interessato né un titolare del trattamento, un responsabile del trattamento o un dipendente. Ad esempio, il titolare del trattamento può assumere un responsabile del trattamento e incaricarlo di trasferire dati personali a terzi. Tale terzo sarà quindi considerato titolare a tutti gli effetti del trattamento che effettua per le proprie finalità. Va notato che, all'interno di un gruppo di società, una società diversa da quella del titolare del trattamento o del responsabile del trattamento è un terzo, anche se appartiene al medesimo gruppo al quale appartiene la società che agisce in qualità di titolare o di responsabile del trattamento.

Esempio: servizi di pulizia

La società A stipula un contratto con un'impresa di servizi di pulizia per i propri uffici. Gli addetti alle pulizie non sono tenuti ad accedere ai dati personali o a trattarli. Anche se occasionalmente possono venire in contatto con i dati quando operano all'interno dell'ufficio, essi possono svolgere i compiti loro assegnati senza accedervi e per contratto è fatto loro divieto di accedere ai dati personali che la società A detiene in quanto titolare del trattamento o di trattarli in qualsivoglia modalità. Gli addetti alle pulizie non sono dipendenti dalla società A né sotto la diretta autorità di quest'ultima. Non vi è alcuna intenzione di ricorrere all'impresa di servizi di pulizia o ai suoi dipendenti per trattare dati personali per conto della società A. L'impresa di servizi di pulizia e i relativi dipendenti devono pertanto essere considerati terzi e il titolare del trattamento deve assicurare l'esistenza di misure di sicurezza adeguate atte a impedire l'accesso ai dati e stabilire un obbligo di riservatezza in caso di accesso accidentale a tali dati.

Esempio: gruppi di società – società capogruppo e controllate

Le società X e Y, che fanno parte del gruppo Z, trattano i dati relativi ai rispettivi dipendenti ai fini della gestione delle risorse umane. A un certo punto, la società capogruppo ZZ decide di richiedere i dati dei dipendenti a tutte le controllate, al fine di elaborare statistiche a livello di gruppo. Nel trasferire dati dalle società X e Y a ZZ, quest'ultima deve essere considerata come terzo, indipendentemente dal fatto che tutte le società facciano parte del medesimo gruppo. La società ZZ sarà considerata titolare del trattamento dei dati a fini statistici.

Destinatario

90. L'articolo 4, paragrafo 9, definisce destinatario la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Le autorità pubbliche non vanno tuttavia considerate destinatari quando ricevono dati personali nell'ambito di un'indagine specifica, conformemente al diritto dell'Unione o degli Stati membri (ad esempio autorità fiscali e doganali, squadre di indagine finanziaria ecc.)[35].

91. La definizione corrisponde in linea generale a quella precedente di «destinatario» di cui alla direttiva 95/46/CE.

92. La definizione si applica a chiunque riceva dati personali, che si tratti o meno di terzi. Ad esempio, quando un titolare del trattamento invia dati personali a un altro soggetto, a un responsabile del trattamento o a terzi, tale soggetto è un destinatario. Un terzo destinatario è considerato titolare di qualsivoglia trattamento che effettua per le proprie finalità dopo aver ricevuto i dati.

Esempio: comunicazione di dati tra società

L'agenzia di viaggi ExploreMore organizza viaggi su richiesta di singoli clienti. Nell'ambito di tale servizio, invia i dati personali dei clienti a compagnie aeree, ad alberghi e alle agenzie che organizzano escursioni affinché possano erogare i rispettivi servizi. ExploreMore, gli alberghi, le compagnie aeree e i fornitori di servizi di escursione sono considerati titolari del trattamento da essi effettuato nell'ambito dei rispettivi servizi. Non esiste alcun rapporto titolare-responsabile. Tuttavia, le compagnie aeree, gli alberghi e i fornitori di servizi di escursione vanno considerati destinatari quando ricevono dati personali da ExploreMore.

PARTE II – CONSEGUENZE DERIVANTI DAI DIVERSI RUOLI ATTRIBUITI

1. RAPPORTO TRA TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO

93. Un'innovazione distintiva introdotta dal GDPR è costituita dalle disposizioni che impongono obblighi direttamente ai responsabili del trattamento. Ad esempio, un responsabile del trattamento deve garantire che le persone autorizzate a trattare i dati personali si siano impegnate alla riservatezza (articolo 28, paragrafo 3), deve tenere un registro di tutte le categorie di attività relative al trattamento (articolo 30, paragrafo 2) e attuare misure tecniche e organizzative adeguate (articolo 32). A determinate condizioni (articolo 37) il responsabile del trattamento deve inoltre designare un responsabile della protezione dei dati e ha il dovere di informare il titolare del trattamento, senza ingiustificato ritardo, dopo essere venuto a conoscenza di una violazione dei dati personali (articolo 33, paragrafo 2). Inoltre, le norme sui trasferimenti di dati verso paesi terzi (capo V) si applicano sia ai responsabili sia ai titolari del trattamento. A tale riguardo, l'EDPB ritiene che l'articolo 28, paragrafo 3, del GDPR, pur conferendo un contenuto specifico al contratto che deve essere stipulato tra il titolare e il responsabile del trattamento, imponga a quest'ultimo obblighi diretti, ivi compreso il dovere di assistere il titolare del trattamento nel garantire la conformità alle disposizioni del regolamento[36].

1.1 SCELTA DEL RESPONSABILE DEL TRATTAMENTO

94. Il titolare del trattamento ha il **dovere di impiegare «unicamente responsabili del trattamento che presentino garanzie sufficienti** per mettere in atto misure tecniche e organizzative adeguate», in modo tale che il trattamento soddisfi i requisiti del GDPR, anche in merito alla sicurezza dello stesso, e garantisca la tutela dei diritti degli interessati[37]. Il titolare del trattamento è pertanto responsabile della valutazione dell'adeguatezza delle garanzie pre-

sentate dal responsabile del trattamento e dovrebbe essere in grado di dimostrare di aver preso in seria considerazione tutti gli elementi di cui al GDPR.

95. Le garanzie «presentate» dal responsabile del trattamento sono quelle che il responsabile del trattamento è in grado di **dimostrare in modo soddisfacente al titolare del trattamento**, essendo queste le uniche che possono essere effettivamente prese in considerazione da detto titolare nel valutare l'adempimento dei suoi obblighi. Spesso ciò richiederà uno scambio di documentazione pertinente (ad esempio, politica in materia di privacy, condizioni di erogazione del servizio, registro delle attività di trattamento, meccanismi di gestione dei log, politica in materia di sicurezza delle informazioni, relazioni di audit esterni sulla protezione dei dati e certificazioni internazionali riconosciute, come la serie ISO 27000).

96. La valutazione della sufficienza delle garanzie da parte del titolare del trattamento è una forma di valutazione del rischio che dipenderà in larga misura dal tipo di trattamento affidato al responsabile e va effettuata caso per caso, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi per i diritti e le libertà delle persone fisiche. Di conseguenza, l'EDPB non può fornire un elenco esaustivo dei documenti o delle attività che il responsabile del trattamento è tenuto a presentare o a dimostrare in un dato caso, in quanto ciò dipende in larga misura dalle circostanze specifiche del trattamento.

97. Il titolare del trattamento dovrebbe tenere conto dei seguenti elementi[38], al fine di valutare l'adeguatezza delle garanzie: le **conoscenze specialistiche** (ad esempio, le competenze tecniche in materia di misure di sicurezza e di violazione dei dati), l'**affidabilità** e le **risorse** del responsabile del trattamento. Anche la reputazione del responsabile del trattamento sul mercato può essere un fattore pertinente di cui i titolari del trattamento possono tenere conto.

98. Inoltre, l'adesione a un codice di condotta o a un meccanismo di certificazione approvato può essere utilizzata come elemento in grado di dimostrare garanzie sufficienti[39]. Si consiglia pertanto ai responsabili del trattamento di informare il titolare del trattamento in merito a detta circostanza e a qualsiasi modifica intervenuta in rapporto alla suddetta adesione.

99. L'obbligo di impiegare solo responsabili del trattamento «che presentano garanzie sufficienti», ai sensi dell'articolo 28, paragrafo 1, del GDPR è un obbligo permanente. Esso non viene meno laddove il titolare e il responsabile del trattamento concludano un contratto o un atto giuridico di altra natura. A intervalli adeguati, il titolare del trattamento dovrebbe verificare le garanzie offerte dal responsabile del trattamento, anche mediante attività di revisione e ispezioni, se del caso[40].

1.2 FORMA DEL CONTRATTO O DELL'ATTO GIURIDICO DI ALTRA NATURA

100. Qualsivoglia trattamento di dati personali da parte di un responsabile del trattamento deve essere disciplinato da un contratto o altro atto giuridico,

a norma del diritto dell'Unione o degli Stati membri, concluso tra il titolare e il responsabile del trattamento, conformemente all'articolo 28, paragrafo 3, del GDPR.

101. Tale atto giuridico deve essere **per iscritto, anche in formato elettronico**[41]. Pertanto, gli accordi non scritti (indipendentemente dalla completezza o dall'efficacia) non possono essere considerati sufficienti per soddisfare i requisiti di cui all'articolo 28 del GDPR. Per evitare difficoltà nel dimostrare che il contratto o altro atto giuridico è effettivamente in vigore, l'EDPB raccomanda di accertarsi che le firme necessarie vi siano incluse, in linea con il diritto applicabile (ad esempio, il diritto contrattuale).

102. Inoltre, ai sensi del diritto dell'Unione o degli Stati membri il contratto o l'altro atto giuridico deve **vincolare il responsabile del trattamento** nei confronti del titolare del trattamento, ovverosia deve definire obblighi vincolanti in capo al responsabile del trattamento, conformemente al diritto dell'UE o degli Stati membri. Deve altresì definire gli obblighi del titolare del trattamento. Nella maggior parte dei casi vi sarà un contratto, tuttavia il regolamento fa riferimento altresì ad un «altro atto giuridico», come il diritto nazionale (primario o derivato) o un altro strumento giuridico. Se l'atto giuridico non prevede tutti i contenuti minimi richiesti, deve essere integrato da un contratto o da un altro atto giuridico che contenga gli elementi mancanti.

103. Poiché il regolamento stabilisce con chiarezza l'obbligo di stipulare un contratto scritto, qualora non sia in vigore nessun altro atto giuridico pertinente si ha una violazione del GDPR[42]. Sia il titolare sia il responsabile del trattamento hanno la responsabilità di garantire l'esistenza di un contratto o di un altro atto giuridico che disciplini il trattamento[43]. Fatte salve le disposizioni di cui all'articolo 83 del GDPR, l'autorità di controllo competente potrà infliggere una sanzione amministrativa pecuniaria sia al titolare sia al responsabile del trattamento, tenendo conto delle circostanze di ogni singolo caso. I contratti stipulati prima della data di applicazione del GDPR dovrebbero essere stati aggiornati ai sensi dell'articolo 28, paragrafo 3. L'assenza di tale aggiornamento, inteso ad allineare un contratto precedentemente esistente ai requisiti del GDPR, costituisce una violazione dell'articolo 28, paragrafo 3.

    Un contratto scritto a norma dell'articolo 28, paragrafo 3, del GDPR può essere integrato in un contratto più ampio, come un accordo sul livello dei servizi. Al fine di agevolare la dimostrazione della conformità al GDPR, l'EDPB raccomanda che gli elementi del contratto volti a dare attuazione all'articolo 28 del GDPR siano chiaramente identificati come tali in un unico punto (ad esempio in un allegato).

104. Per adempiere all'obbligo di stipula di un contratto, **il titolare e il responsabile del trattamento possono scegliere di negoziarne uno proprio**, ivi compresi tutti gli elementi obbligatori, **o di basarsi, in tutto o in parte, su clausole contrattuali tipo in relazione agli obblighi di cui all'articolo 28**[44].

105. Una serie di clausole contrattuali tipo (SCC) può essere adottata in alterna-

tiva dalla Commissione[45] o da un'autorità di controllo, conformemente al meccanismo di coerenza[46]. Tali clausole potrebbero far parte di una certificazione rilasciata al titolare o al responsabile del trattamento, ai sensi degli articoli 42 o 43[47].

106. L'EDPB desidera chiarire che non vi è alcun obbligo in capo ai titolari e ai responsabili del trattamento di stipulare un contratto basato su SCC né ciò deve necessariamente avere la precedenza rispetto alla stipula di un contratto ad hoc. Entrambe le opzioni sono ammissibili ai fini dell'adempimento alla normativa in materia di protezione dei dati, a seconda delle circostanze specifiche, purché siano soddisfatti i requisiti di cui all'articolo 28, paragrafo 3.

107. Se le parti desiderano avvalersi delle clausole contrattuali tipo, le clausole di protezione dei dati previste dall'accordo devono essere le stesse delle SCC. Le SCC presenteranno spesso spazi vuoti da compilare od opzioni che le parti devono selezionare. Inoltre, come indicato in precedenza, le SCC saranno generalmente integrate in un accordo più ampio che descriva l'oggetto del contratto, le condizioni finanziarie e le altre clausole concordate: le parti potranno aggiungere ulteriori clausole (ad esempio il diritto applicabile e la giurisdizione), purché non siano in contrasto, direttamente o indirettamente, con le SCC[48] e non pregiudichino la tutela conferita dal GDPR e dalle normative dell'UE o degli Stati membri in materia di protezione dei dati.

108. I contratti tra titolari del trattamento e responsabili del trattamento possono talvolta essere redatti unilateralmente da una delle parti. Diversi fattori possono determinare la parte o le parti che redige/redigono il contratto, tra cui: posizionamento sul mercato e potere contrattuale, le competenze tecniche e l'accesso a servizi giuridici. Ad esempio, alcuni fornitori di servizi tendono a stabilire termini e condizioni standard, tra cui accordi di trattamento dei dati.

109. Un accordo tra il titolare e il responsabile del trattamento deve rispettare i requisiti di cui all'articolo 28 del GDPR, al fine di garantire che il responsabile tratti i dati personali in conformità con lo stesso GDPR. Qualsivoglia accordo di questo tipo dovrebbe tenere conto delle responsabilità specifiche dei titolari e dei responsabili del trattamento. Sebbene l'articolo 28 preveda un elenco di elementi che devono essere contemplati in ogni contratto che disciplini il rapporto tra titolari e responsabili del trattamento, esso lascia margini di negoziato tra le parti di tali contratti. In talune situazioni il titolare o il responsabile del trattamento godono di un minore potere negoziale ai fini di una personalizzazione dell'accordo sulla protezione dei dati. Il ricorso alle clausole contrattuali tipo adottate a norma dell'articolo 28 (paragrafi 7 e 8) può contribuire a riequilibrare le posizioni negoziali e a garantire che i contratti rispettino il GDPR.

110. Il fatto che il contratto e le condizioni commerciali in esso dettagliate siano redatti dal prestatore di servizi piuttosto che dal titolare del trattamento non è di per sé problematico e non costituisce di per sé una ragione suffi-

ciente per concludere che il prestatore di servizi debba essere considerato titolare del trattamento. Inoltre, lo squilibrio di potere contrattuale tra un piccolo titolare del trattamento e grandi fornitori di servizi non dovrebbe essere considerato una giustificazione per l'accettazione, da parte del suddetto titolare, di clausole e di condizioni contrattuali non conformi alla normativa in materia di protezione dei dati né può esonerarlo dai relativi obblighi. Il titolare del trattamento deve valutare i termini contrattuali e, nella misura in cui li accetta liberamente e si avvale del servizio, assumersi altresì la piena responsabilità del rispetto del GDPR. Qualsivoglia proposta di modifica, da parte di un responsabile del trattamento, degli accordi di trattamento dei dati di cui alle condizioni generali di contratto dovrebbe essere notificata e approvata direttamente dal titolare del trattamento, tenendo conto del margine di discrezionalità di cui il responsabile del trattamento dispone in merito agli elementi non essenziali dei mezzi (cfr. paragrafi 40-41 che precedono). La mera pubblicazione di tali modifiche sul sito web del responsabile del trattamento non è conforme all'articolo 28.

1.3 CONTENUTO DEL CONTRATTO O ALTRO ATTO GIURIDICO

111. Prima di esaminare nel dettaglio i singoli requisiti specifici definiti dal GDPR rispetto al contenuto del contratto o di un altro atto giuridico, occorre svolgere alcune osservazioni di natura generale.

112. Se è vero che gli elementi di cui all'articolo 28 del regolamento ne costituiscono il contenuto essenziale, il contratto dovrebbe essere uno strumento con cui il titolare e il responsabile del trattamento possono chiarire ulteriormente in che modo detti elementi essenziali saranno attuati mediante istruzioni dettagliate. Pertanto, **l'accordo relativo al trattamento dovrebbe non già meramente ribadire le disposizioni del GDPR**, bensì prevedere informazioni più specifiche e concrete sul modo in cui saranno soddisfatti i requisiti e sul livello di sicurezza previsto per il trattamento dei dati personali oggetto dell'accordo. Lungi dall'essere un esercizio formalistico, la negoziazione e la stipula del contratto sono un'opportunità per specificare i dettagli relativi al trattamento[49]. In effetti, ai sensi del GDPR, la «protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento [...] esigono una chiara ripartizione delle responsabilità[50]».

113. Nel contempo, il contratto dovrebbe **tener conto *«dei compiti e responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato»*[51]**. In linea generale, il contratto tra le parti dovrebbe essere redatto tenendo conto della specifica attività di trattamento dei dati. Ad esempio, non è necessario imporre tutele e procedure particolarmente rigorose a un responsabile del trattamento preposto a un'attività di trattamento che presenta solo rischi minori: sebbene ciascun responsabile del trattamento sia tenuto a rispettare i requisiti di cui al regolamento, le misure e le procedure dovrebbero essere calibrate in base alla situazione specifica. In

ogni caso, il contratto deve contemplare tutti gli elementi di cui all'articolo 28, paragrafo 3. Nel contempo, dovrebbe prevedere taluni elementi che possano aiutare il responsabile del trattamento a comprendere i rischi per i diritti e le libertà degli interessati insiti nel trattamento: poiché l'attività è svolta per conto del titolare, spesso quest'ultimo ha una comprensione più approfondita dei rischi che il trattamento comporta dal momento che è a conoscenza delle circostanze in cui avviene.

114. Quanto al contenuto obbligatorio del contratto o di altro atto giuridico, l'EDPB interpreta l'articolo 28, paragrafo 3, in modo tale per cui deve esservi stabilito:

- l'**oggetto** del trattamento (ad esempio, registrazioni di videosorveglianza di persone che entrano o escono da una struttura ad alta sicurezza). Sebbene sia un concetto ampio, esso deve essere formulato con specifiche sufficienti affinché l'oggetto principale del trattamento sia chiaro;
- la **durata**[52] del trattamento: occorre specificare il periodo di tempo esatto o i criteri utilizzati per determinarlo; ad esempio, si potrebbe fare riferimento alla durata dell'accordo relativo al trattamento;
- la **natura** del trattamento: il tipo di operazioni eseguite nell'ambito del trattamento (ad esempio: «ripresa», «registrazione», «archiviazione di immagini» ecc.) e la finalità del trattamento (ad esempio: la rilevazione degli ingressi illegittimi). Tale descrizione dovrebbe essere la più completa possibile, a seconda dell'attività di trattamento specifica, in modo da consentire a soggetti esterni (ad esempio le autorità di controllo) di comprendere il contenuto e i rischi del trattamento affidato al relativo responsabile;
- la **tipologia di dati personali**: questo elemento dovrebbe essere specificato nel modo più dettagliato possibile (ad esempio: le immagini video delle persone che entrano ed escono dalla struttura). Non sarebbe sufficiente limitarsi a specificare che si tratta di «dati personali, ai sensi dell'articolo 4, paragrafo 1, del GDPR» o «di categorie particolari di dati personali, ai sensi dell'articolo 9». Nel caso di categorie particolari di dati, il contratto o l'atto giuridico dovrebbero specificare almeno i tipi di dati in questione, ad esempio «informazioni relative alle cartelle cliniche» o «informazioni sull'appartenenza dell'interessato a un sindacato»;
- le **categorie di interessati**: anche questo aspetto dovrebbe essere indicato in modo piuttosto specifico (ad esempio: «visitatori», «dipendenti», servizi di consegna ecc.);
- gli **obblighi e i diritti del titolare del trattamento**: tali diritti sono esaminati ulteriormente nelle sezioni successive (ad esempio, per quanto riguarda il diritto del titolare del trattamento di effettuare ispezioni e attività di revisione). Quanto agli obblighi del titolare del trattamento, tra gli esempi figurano quello di fornire al responsabile del trattamento i dati di cui al contratto, di fornire e documentare qualsivoglia istruzione relativa al trattamento dei dati da parte del responsabile del trattamento, di garantire, prima e durante l'intero corso del trattamento, l'adempimento degli obblighi di cui al GDPR posti in capo al responsabile, di controllare detto trattamento anche mediante attività di revisione e ispezioni unitamente al suddetto responsabile.

115. Sebbene il GDPR elenchi gli elementi che vanno sempre inclusi nell'accordo, può essere necessario prevedere altre informazioni pertinenti, in funzione del contesto e dei rischi posti dal trattamento nonché di eventuali ulteriori requisiti applicabili.

1.3.1 OBBLIGO DEL RESPONSABILE DEL TRATTAMENTO DI TRATTARE I DATI SOLO SU ISTRUZIONE DOCUMENTATA DEL TITOLARE DEL TRATTAMENTO (ARTICOLO 28, PARAGRAFO 3, LETTERA A) DEL GDPR)

116. La necessità di specificare tale obbligo deriva dal fatto che il responsabile del trattamento tratta i dati per conto del titolare. I titolari del trattamento devono fornire ai responsabili istruzioni relative a ciascuna attività di trattamento. Tali istruzioni possono riguardare trattamenti ammessi e quelli vietati, procedure più dettagliate, la modalità di messa in sicurezza dei dati, ecc. Il responsabile si limita a quanto disposto dal titolare del trattamento, ma ha la possibilità di suggerire elementi che, se accettati dal titolare del trattamento, diventano parte delle istruzioni impartite.

117. Quando un responsabile tratta i dati non limitandosi alle istruzioni del titolare del trattamento, e ciò equivale a una decisione che determina le finalità e i mezzi dello stesso, il suddetto responsabile è in violazione dei propri obblighi e può anche essere considerato titolare di tale trattamento, ai sensi dell'articolo 28, paragrafo 10 (cfr. infra, sottosezione 1.5)[53].

118. Le istruzioni impartite dal titolare del trattamento devono essere **documentate**. A tal fine, si raccomanda di prevedere una procedura e un modello per fornire ulteriori istruzioni attraverso un allegato al contratto o altro atto giuridico. In alternativa, le istruzioni possono essere impartite in qualsiasi forma scritta (ad esempio per posta elettronica) e in qualsivoglia altra forma documentata, purché sia possibile documentarle. In ogni caso, per evitare difficoltà nel dimostrare che le istruzioni del titolare del trattamento sono state debitamente documentate, l'EDPB raccomanda di accorpare tali istruzioni al contratto o al diverso atto giuridico.

119. L'obbligo in capo al responsabile del trattamento di astenersi da qualsivoglia attività di trattamento non basata sulle istruzioni del titolare si applica anche ai **trasferimenti** di dati personali verso un paese terzo o un'organizzazione internazionale. Il contratto dovrebbe specificare i requisiti per i trasferimenti verso paesi terzi o organizzazioni internazionali tenendo conto delle disposizioni di cui al capo V del GDPR.

120. L'EDPB raccomanda al titolare del trattamento di prestare la dovuta attenzione a questo punto specifico, in particolare laddove il responsabile deleghi talune attività di trattamento ad altri responsabili e laddove abbia divisioni o unità ubicate in paesi terzi. Se le istruzioni del titolare del trattamento non consentono trasferimenti o comunicazioni verso paesi terzi, il responsabile non sarà autorizzato ad assegnare il trattamento a un sub-responsabile in un paese terzo né potrà far trattare i dati in una sua divisione non ubicata nell'UE.

121. Un responsabile del trattamento può trattare dati in modo difforme dalle istruzioni documentate del titolare **laddove sia tenuto a trattare e/o a trasferire dati personali ai sensi del diritto dell'UE o del diritto dello Stato membro cui il responsabile del trattamento è soggetto**. Tale disposizione rivela inoltre l'importanza di negoziare e di redigere con attenzione gli accordi di trattamento dei dati, in quanto, ad esempio, può avvenire che una delle parti necessiti di una consulenza legale in merito alla sussistenza di un siffatto obbligo giuridico. Ciò deve avvenire tempestivamente, in quanto il responsabile del trattamento ha l'obbligo di informare il titolare in merito all'esistenza di un obbligo del genere prima di iniziare il trattamento stesso. Tale obbligo di informazione non sussiste solo laddove il diritto stesso (dell'UE o dello Stato membro) vieti al responsabile del trattamento di informare il titolare in merito a «rilevanti motivi di interesse pubblico». In ogni caso, qualsivoglia trasferimento o comunicazione può aver luogo solo se autorizzato dal diritto dell'Unione, anche in conformità all'articolo 48 del GDPR.

1.3.2 OBBLIGO DEL RESPONSABILE DEL TRATTAMENTO DI GARANTIRE CHE LE PERSONE AUTORIZZATE A TRATTARE I DATI PERSONALI SI SIANO IMPEGNATE ALLA RISERVATEZZA O ABBIANO UN ADEGUATO OBBLIGO LEGALE DI RISERVATEZZA (ARTICOLO 28, PARAGRAFO 3, LETTERA B) DEL GDPR)

122. Il contratto deve prevedere l'obbligo in capo al responsabile del trattamento di garantire che chiunque quest'ultimo autorizzi a trattare dati personali sia tenuto alla riservatezza. Ciò può avvenire mediante un accordo contrattuale specifico o in forza degli obblighi di legge già in vigore.

123. Il concetto ampio di «persone autorizzate a trattare i dati personali» contempla i lavoratori dipendenti e temporanei. In linea generale, il responsabile del trattamento dovrebbe mettere i dati personali a disposizione solo dei dipendenti che ne hanno effettivamente bisogno per svolgere i compiti per i quali il responsabile è stato incaricato dal titolare del trattamento.

124. L'impegno o l'obbligo di riservatezza deve essere «adeguato», ovverosia esso deve vietare effettivamente alla persona autorizzata di divulgare informazioni riservate senza autorizzazione e deve essere sufficientemente ampio da comprendere tutti i dati personali trattati per conto del titolare del trattamento nonché le condizioni alle quali tali dati sono trattati.

1.3.3 OBBLIGO DEL RESPONSABILE DEL TRATTAMENTO DI ADOTTARE TUTTE LE MISURE RICHIESTE A NORMA DELL'ARTICOLO 32 (ARTICOLO 28, PARAGRAFO 3, LETTERA C) DEL GDPR)

125. L'articolo 32 impone al titolare e al responsabile del trattamento di mettere in atto misure tecniche e organizzative di sicurezza adeguate. Sebbene tale obbligo sia già direttamente imposto al responsabile del trattamento i cui trattamenti rientrano nell'ambito di applicazione del GDPR, l'obbligo

a norma dell'articolo 32 di adottare tutte le misure richieste deve comunque figurare nel contratto relativo alle attività di trattamento affidate dal titolare.

126. Come già rilevato, il contratto relativo al trattamento non dovrebbe limitarsi a ribadire le disposizioni del GDPR. È necessario che il contratto preveda o faccia riferimento alle misure di sicurezza da adottare, **all'obbligo in capo al responsabile del trattamento di ottenere l'approvazione del titolare del trattamento prima di apportare modifiche** e a un riesame periodico delle misure di sicurezza, al fine di garantirne l'adeguatezza rispetto ai rischi, che può cambiare nel tempo. Ai sensi dell'articolo 32, paragrafo 1, del GDPR le informazioni relative alle misure di sicurezza da includere nel contratto devono essere sufficientemente dettagliate da consentire al titolare del trattamento di valutare l'adeguatezza delle misure stesse. Inoltre, la descrizione è necessaria anche per consentire al titolare del trattamento di adempiere al proprio obbligo in materia di responsabilizzazione, a norma dell'articolo 5, paragrafo 2, e dell'articolo 24 del GDPR, per quanto concerne le misure di sicurezza imposte al responsabile del trattamento. Un obbligo corrispondente cui è soggetto il responsabile del trattamento, quello di assistere il titolare del trattamento e di mettere a disposizione tutte le informazioni necessarie per dimostrare la conformità al regolamento, può essere desunto dall'articolo 28, paragrafo 3, lettere f) e h), del GDPR.

127. Il livello di istruzioni fornite dal titolare al responsabile del trattamento in merito alle misure da attuare dipende dalle circostanze specifiche. In taluni casi, il titolare del trattamento può fornire una descrizione chiara e dettagliata delle misure di sicurezza da attuare. In altri casi, può definire gli obiettivi minimi di sicurezza da conseguire, chiedendo al responsabile del trattamento di proporre l'attuazione di misure di sicurezza specifiche. In ogni caso, il titolare deve fornire al responsabile del trattamento una descrizione delle attività di trattamento e degli obiettivi di sicurezza (sulla base della valutazione del rischio eseguita dallo stesso titolare) nonché approvare le misure proposte dal responsabile del trattamento. Quanto sopra potrebbe essere incluso in un allegato al contratto. Il titolare del trattamento esercita il proprio potere decisionale sulle caratteristiche principali delle misure di sicurezza, sia elencandole esplicitamente sia approvando quelle proposte dal responsabile del trattamento.

1.3.4 OBBLIGO DEL RESPONSABILE DEL TRATTAMENTO DI RISPETTARE LE CONDIZIONI DI CUI ALL'ARTICOLO 28, PARAGRAFO 2, E ALL'ARTICOLO 28, PARAGRAFO 4, PER RICORRERE A UN ALTRO RESPONSABILE DEL TRATTAMENTO (ARTICOLO 28, PARAGRAFO 3, LETTERA D) DEL GDPR)

128. L'accordo deve specificare che il responsabile del trattamento non può ricorrere a un altro responsabile del trattamento senza previa autorizzazione scritta del titolare e indicare se detta autorizzazione abbia natura specifica o generica. In caso di autorizzazione generica, il responsabile del

trattamento è tenuto a informare il titolare in merito a qualsivoglia modifica riguardante il sub-responsabile del trattamento ai sensi di un'autorizzazione scritta e a dare al titolare del trattamento la possibilità di opporsi. Si raccomanda che il contratto definisca la procedura a tal fine. Va osservato che il dovere del responsabile di informare il titolare di qualsivoglia modifica relativa a sub-responsabili del trattamento implica che il responsabile del trattamento comunichi o segnali attivamente tali modifiche al titolare[54]. Inoltre, qualora sia richiesta un'autorizzazione specifica, il contratto dovrebbe definire la procedura per ottenere detta autorizzazione.

129. Quando il responsabile del trattamento ricorre a un altro responsabile del trattamento, tra di essi deve essere concluso un contratto che imponga i medesimi obblighi in materia di protezione dei dati che figurano in capo al responsabile del trattamento originario; in alternativa, tali obblighi devono essere imposti da un altro atto giuridico, ai sensi del diritto dell'Unione o dello Stato membro (cfr. anche il paragrafo 160). Ciò include l'obbligo ai sensi dell'articolo 28, paragrafo 3, lettera h), di consentire e contribuire alle attività di revisione da parte del titolare del trattamento o di un altro soggetto da questi incaricato[55]. Sul responsabile del trattamento incombe la responsabilità, nei confronti del titolare del trattamento, di assicurare il rispetto degli obblighi in materia di protezione dei dati da parte degli altri sub-responsabili del trattamento (per ulteriori dettagli sul contenuto raccomandato per l'accordo, cfr. la sottosezione 1.6 in appresso)[56].

1.3.5 OBBLIGO DEL RESPONSABILE DEL TRATTAMENTO DI ASSISTERE IL TITOLARE DEL TRATTAMENTO NELL'ADEMPIMENTO DELL'OBBLIGO DI DARE SEGUITO ALLE RICHIESTE PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO (ARTICOLO 28, PARAGRAFO 3, LETTERA E), DEL GDPR)

130. Pur stipulando che dare seguito alle richieste degli interessati sia di competenza del titolare del trattamento, il contratto deve prevedere che il responsabile del trattamento abbia l'obbligo di fornire assistenza «con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile». La natura di tale assistenza può variare notevolmente «tenendo conto della natura del trattamento» e a seconda del tipo di attività affidata al responsabile. I dettagli relativi all'assistenza che il responsabile del trattamento è tenuto a fornire dovrebbero essere previsti nel contratto o in un suo allegato.

131. Mentre l'assistenza in questione può consistere semplicemente nel trasmettere tempestivamente qualsiasi richiesta ricevuta e/o nel consentire al titolare del trattamento di estrarre e gestire direttamente i dati personali pertinenti, in talune circostanze al responsabile saranno affidati compiti tecnici più specifici, in particolare laddove sia in grado di estrarre e gestire i dati personali.

132. È fondamentale tenere presente che, sebbene la gestione pratica delle singole richieste possa essere esternalizzata al responsabile del trattamento,

è al titolare che spetta soddisfarle. Pertanto, la valutazione dell'ammissibilità delle richieste degli interessati e/o del rispetto dei requisiti di cui al GDPR dovrebbe essere effettuata dal titolare del trattamento, caso per caso o mediante istruzioni chiare fornite al responsabile per mezzo del contratto prima dell'inizio del trattamento. Inoltre, i termini di cui al capo III non possono essere prorogati dal titolare sulla base del fatto che le informazioni necessarie devono essere fornite dal responsabile del trattamento.

1.3.6 OBBLIGO DEL RESPONSABILE DEL TRATTAMENTO DI ASSISTERE IL TITOLARE DEL TRATTAMENTO NEL GARANTIRE IL RISPETTO DEGLI OBBLIGHI DI CUI AGLI ARTICOLI DA 32 A 36 (ARTICOLO 28, PARAGRAFO 3, LETTERA F), DEL GDPR)

133. È necessario che il contratto eviti semplicemente di ribadire tali funzioni di assistenza: **l'accordo dovrebbe contenere informazioni dettagliate sulle modalità con le quali al responsabile del trattamento è richiesto di assistere il titolare nell'adempiere agli obblighi elencati**. Ad esempio, negli allegati all'accordo possono essere aggiunti moduli e procedure che consentano al responsabile del trattamento di fornire al titolare tutte le informazioni necessarie.

134. Il tipo e il grado di assistenza che il responsabile del trattamento è tenuto a fornire possono variare notevolmente *«tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento»*. Il titolare deve informare adeguatamente il responsabile del trattamento in merito ai rischi di quest'ultimo e a qualsiasi altra circostanza che possa aiutare il responsabile del trattamento a svolgere i propri compiti.

135. Passando agli obblighi specifici, il responsabile del trattamento ha innanzitutto il dovere di assistere il titolare nell'adempimento dell'obbligo di adottare misure tecniche e organizzative adeguate per garantire la sicurezza del trattamento[57]. Sebbene in una certa misura ciò possa coincidere con il requisito che il responsabile del trattamento stesso adotti misure di sicurezza adeguate qualora le operazioni di trattamento da questi svolte rientrino nell'ambito di applicazione del GDPR, si tratta cionondimeno di due obblighi distinti, in quanto uno si riferisce alle misure del responsabile e l'altro riguarda quelle del titolare del trattamento.

136. In secondo luogo, il responsabile del trattamento deve assistere il titolare nell'adempimento dell'obbligo di notificare le violazioni dei dati personali all'autorità di controllo e agli interessati. Il responsabile del trattamento deve informare il titolare ogniqualvolta rilevi una violazione dei dati personali che interessa le strutture o i sistemi informatici del responsabile o di un sub-responsabile del trattamento e deve aiutare il titolare del trattamento a ottenere le informazioni da comunicare nella notifica all'autorità di controllo[58]. Il GDPR prevede che il titolare del trattamento notifichi una violazione senza indebito ritardo, al fine di ridurre al minimo il danno per le persone fisiche e di massimizzare la possibilità di porre rimedio alla violazione in modo adeguato. Pertanto, la notifica da parte del responsabile al

titolare del trattamento dovrebbe avvenire senza indebiti ritardi[59]. In base alle caratteristiche specifiche del trattamento affidato al responsabile, può essere opportuno che le parti includano nel contratto un lasso di tempo specifico (ad esempio, il numero di ore) entro il quale il responsabile del trattamento informa il titolare nonché il punto di contatto per tali notifiche, le relative modalità e il contenuto minimo previsto dal titolare del trattamento[60]. L'accordo contrattuale tra il titolare e il responsabile del trattamento può altresì autorizzare il responsabile a segnalare direttamente una violazione dei dati, ai sensi degli articoli 33 e 34; tuttavia, l'obbligo legale della notifica resta in capo al titolare del trattamento[61]. Se il responsabile del trattamento notifica una violazione direttamente all'autorità di controllo e ne informa gli interessati, conformemente agli articoli 33 e 34, tale responsabile deve informarne anche il titolare del trattamento e fornirgli copia della notifica e delle informazioni.

137. Inoltre, il responsabile del trattamento deve assistere il titolare anche nello svolgimento di valutazioni d'impatto sulla protezione dei dati, se necessario, e nella consultazione dell'autorità di controllo qualora il risultato di tali valutazioni indichi la sussistenza di un rischio elevato che non può essere attenuato.

138. L'obbligo di assistenza non può consistere in un trasferimento della responsabilità, in quanto gli obblighi in questione sono imposti al titolare del trattamento. Ad esempio, sebbene la valutazione d'impatto sulla protezione dei dati possa essere effettuata in concreto da un responsabile del trattamento, in capo al titolare permane il dovere di effettuare la valutazione[62] e il responsabile del trattamento è tenuto solo ad assistere il titolare «se necessario e su richiesta»[63]. Di conseguenza, è il titolare del trattamento (e non il responsabile) che deve prendere l'iniziativa di effettuare la valutazione d'impatto sulla protezione dei dati.

1.3.7 OBBLIGO DEL RESPONSABILE DEL TRATTAMENTO, AL TERMINE DELLA RELATIVA ATTIVITÀ, DI CANCELLARE O RESTITUIRE, SU SCELTA DEL TITOLARE DEL TRATTAMENTO, TUTTI I DATI PERSONALI AL TITOLARE DEL TRATTAMENTO E CANCELLARE LE COPIE ESISTENTI (ARTICOLO 28, PARAGRAFO 3, LETTERA G), DEL GDPR)

139. I termini contrattuali sono intesi a garantire che i dati personali siano oggetto di una protezione adeguata dopo la fine della «prestazione di servizi relativi al trattamento»: spetta pertanto al titolare decidere cosa il responsabile del trattamento debba fare in relazione ai dati personali.

140. Il titolare del trattamento può inizialmente decidere in merito alla cancellazione o alla restituzione dei dati personali, specificandolo nel contratto, mediante una comunicazione scritta da inviare tempestivamente al responsabile del trattamento. Il contratto o altro atto giuridico dovrebbe prevedere la possibilità per il titolare del trattamento di modificare la scelta operata prima della fine della prestazione dei servizi relativi al tratta-

mento. Il contratto dovrebbe inoltre specificare la procedura per fornire tali istruzioni.

141. Se il titolare del trattamento sceglie di cancellare i dati personali, il responsabile del trattamento dovrebbe garantire che la cancellazione sia effettuata in modo sicuro, anche ai fini dell'adempimento dell'articolo 32 del GDPR. Il responsabile dovrebbe confermare al titolare del trattamento che la cancellazione è stata completata entro un termine concordato e secondo modalità convenute.

142. Il responsabile del trattamento deve cancellare tutte le copie esistenti dei dati, salvo che il diritto dell'UE o degli Stati membri non preveda un'ulteriore conservazione. Se il responsabile o il titolare del trattamento sono a conoscenza di tali obblighi di legge, ne informano l'altra parte al più presto.

1.3.8 OBBLIGO DEL RESPONSABILE DEL TRATTAMENTO DI METTERE A DISPOSIZIONE DEL TITOLARE DEL TRATTAMENTO TUTTE LE INFORMAZIONI NECESSARIE PER DIMOSTRARE IL RISPETTO DEGLI OBBLIGHI DI CUI ALL'ARTICOLO 28 E CONSENTIRE E CONTRIBUIRE ALLE ATTIVITÀ DI REVISIONE, COMPRESE LE ISPEZIONI, REALIZZATE DAL TITOLARE DEL TRATTAMENTO O DA UN ALTRO SOGGETTO DA QUESTI INCARICATO (ARTICOLO 28, PARAGRAFO 3, LETTERA H), DEL GDPR)

143. Il contratto deve prevedere disposizioni dettagliate sulla frequenza e sulle modalità del flusso di informazioni tra il responsabile e il titolare del trattamento, in modo tale che il titolare del trattamento sia pienamente informato in merito a quegli elementi del trattamento atti a dimostrare il rispetto degli obblighi di cui all'articolo 28 del GDPR. Ad esempio, le sezioni pertinenti dei registri delle attività di trattamento del responsabile possono essere condivise con il titolare del trattamento. Il responsabile del trattamento dovrebbe fornire tutte le informazioni sulle modalità di effettuazione dei trattamenti svolti per conto del titolare. Tali informazioni dovrebbero includere dettagli sul funzionamento dei sistemi utilizzati, sulle misure di sicurezza, sul modo in cui sono soddisfatti i requisiti di conservazione dei dati, sull'ubicazione e sui trasferimenti dei dati, su chi vi ha accesso e su chi sono i relativi destinatari, sui sub-responsabili ecc.

144. Il contratto deve prevedere ulteriori disposizioni per quanto concerne la facoltà del titolare o di un altro revisore da questi incaricato di svolgere ispezioni e attività di revisione e gli obblighi di contribuire a tali attività.

Il GDPR specifica che le ispezioni e le attività di revisione sono svolte dal titolare del trattamento o da un terzo da questi incaricato. L'obiettivo di dette attività di revisione è garantire che il titolare disponga di tutte le informazioni relative all'attività di trattamento svolta per suo conto e alle garanzie fornite dal responsabile del trattamento[64]. Quest'ultimo può suggerire la scelta di un revisore specifico, tuttavia, ai sensi dell'articolo 28, paragrafo 3, lettera h), del GDPR, la decisione finale è lasciata al titolare

del trattamento. Inoltre, anche se l'ispezione è effettuata da un revisore proposto dal responsabile del trattamento, il titolare si riserva il diritto di contestare la portata, la metodologia e i risultati dell'ispezione[65].

Le parti dovrebbero cooperare in buona fede e valutare se e quando sia necessario effettuare attività di revisione presso il responsabile del trattamento nonché quale tipo di revisione o ispezione (a distanza/in loco/secondo altre modalità utili per raccogliere le informazioni necessarie) sia necessario e appropriato nel caso di specie, tenendo conto altresì delle questioni in materia di sicurezza; la scelta finale in merito spetta al titolare del trattamento. In seguito ai risultati dell'ispezione, il titolare del trattamento dovrebbe avere la facoltà di chiedere al responsabile di adottare misure successive, ad esempio per rimediare alle carenze e alle lacune individuate[66]. Analogamente, dovrebbero essere stabilite procedure specifiche per quanto riguarda l'ispezione dei sub-responsabili del trattamento da parte del responsabile e del titolare del trattamento (cfr. la sottosezione 1.6 in appresso)[67].

145. La questione della ripartizione dei costi tra un titolare e un responsabile del trattamento per quanto riguarda le attività di revisione non è contemplata dal GDPR ed è soggetta a considerazioni di ordine commerciale. Tuttavia, l'articolo 28, paragrafo 3, lettera h), stabilisce che il contratto preveda l'obbligo, in capo al responsabile del trattamento, di mettere a disposizione del titolare tutte le informazioni necessarie nonché l'obbligo di consentire e contribuire alle attività di revisione, ivi comprese le ispezioni, effettuate dal titolare del trattamento o da un altro revisore da esso incaricato. Ciò significa, in pratica, che le parti non dovrebbero inserire nel contratto clausole che prevedano il pagamento di costi o oneri manifestamente sproporzionati o eccessivi, aventi un conseguente effetto dissuasivo su una di esse. Tali clausole implicherebbero infatti che i diritti e gli obblighi di cui all'articolo 28, paragrafo 3, lettera h), non sarebbero mai esercitati nella pratica e diventerebbero puramente teorici, sebbene costituiscano parte integrante delle garanzie in materia di protezione dei dati di cui all'articolo 28 del GDPR.

1.4 ISTRUZIONI CHE VIOLANO LA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI

146. Ai sensi dell'articolo 28, paragrafo 3, il responsabile del trattamento deve informare tempestivamente il titolare del trattamento qualora, a suo avviso, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

147. Di fatto, il responsabile del trattamento ha il dovere di rispettare le istruzioni del titolare del trattamento, ma ha anche l'obbligo generale di rispettare la legge. Un'istruzione che violi la normativa in materia di protezione dei dati causerebbe un conflitto tra i due obblighi di cui sopra.

148. Una volta informato che una delle sue istruzioni potrebbe essere in vio-

lazione del diritto in materia di protezione dei dati, il titolare del trattamento è tenuto a valutare la situazione e a verificare se detta violazione effettivamente sussista.

149. L'EDPB raccomanda alle parti di concordare nel contratto le conseguenze della notifica inviata dal responsabile del trattamento secondo cui una determinata istruzione comporta una violazione della normativa nonché le conseguenze dell'eventuale inerzia da parte del titolare del trattamento in tale contesto. Un esempio potrebbe essere l'inserimento di una clausola sulla risoluzione del contratto se il titolare del trattamento insiste nell'impartire un'istruzione illecita. Un altro esempio potrebbe essere una clausola sulla possibilità per il responsabile del trattamento di sospendere l'attuazione dell'istruzione in questione fino a quando il titolare del trattamento non la confermi, modifichi o ritiri[68].

1.5 RESPONSABILE DEL TRATTAMENTO CHE DETERMINA LE FINALITÀ E I MEZZI DEL TRATTAMENTO

150. Se viola il regolamento nel determinare le finalità e i mezzi del trattamento, il responsabile è considerato titolare del trattamento in questione (articolo 28, paragrafo 10, del GDPR).

1.6 SUB-RESPONSABILI

151. Le attività di trattamento dei dati sono spesso svolte da un gran numero di soggetti e le catene di esternalizzazione diventano sempre più complesse. Il GDPR introduce obblighi specifici che scaturiscono laddove un (sub-) responsabile del trattamento intenda coinvolgere un altro soggetto, aggiungendo in tal modo un altro anello alla catena, affidandogli attività che richiedono il trattamento di dati personali. L'analisi volta a stabilire se il prestatore di servizi agisca in qualità di sub-responsabile dovrebbe essere effettuata in linea con quanto sopra detto sul concetto di responsabile del trattamento (cfr. paragrafo 83).

152. Sebbene la catena possa essere alquanto lunga, il titolare del trattamento mantiene un ruolo centrale nella determinazione della finalità e dei mezzi dello stesso. L'articolo 28, paragrafo 2, del GDPR stabilisce che il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento (anche in formato elettronico). In caso di autorizzazione scritta generale, il responsabile deve informare il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare di cui sopra la possibilità di opporsi a dette modifiche. In entrambi i casi, prima che qualsivoglia trattamento di dati personali sia affidato al sub-responsabile del trattamento, il responsabile deve ottenere l'autorizzazione scritta del titolare dello stesso. Per effettuare la valutazione e decidere se autorizzare o meno tale

ulteriore esternalizzazione, il responsabile del trattamento dovrà fornire al titolare un elenco dei sub-responsabili previsti (contenente, per ciascuno di essi: l'ubicazione, le modalità di esecuzione e la prova delle garanzie messe in atto)[69].

153. La previa autorizzazione scritta di cui sopra può essere specifica, vale a dire riferita a un determinato sub-responsabile per una determinata attività di trattamento e in un momento specifico, o generale. Ciò dovrebbe essere specificato nel contratto o nel diverso atto giuridico disciplinante il trattamento.

154. Qualora il titolare del trattamento decida di accettare determinati sub-responsabili, al momento della firma del contratto è opportuno inserire nello stesso o in un suo allegato un elenco dei sub-responsabili del trattamento approvati. L'elenco dovrebbe quindi essere tenuto aggiornato, conformemente all'autorizzazione generale o specifica concessa dal titolare del trattamento.

155. Se il titolare del trattamento sceglie di concedere un'**autorizzazione specifica** dovrebbe specificare per iscritto a quale sub-responsabile e a quale attività di trattamento fa riferimento. Qualsivoglia modifica successiva richiederà un'ulteriore autorizzazione del titolare del trattamento prima di essere posta in essere. Qualora la richiesta di un'autorizzazione specifica da parte del responsabile del trattamento non riceva risposta entro il termine stabilito, la si considera respinta. Il titolare del trattamento dovrebbe decidere se concedere o meno l'autorizzazione tenendo conto dell'obbligo di ricorrere unicamente a responsabili del trattamento in grado di offrire «garanzie sufficienti» (cfr. la sottosezione 1.1 che precede)[70].

156. In alternativa, il titolare del trattamento può fornire la propria **autorizzazione generale** all'uso di sub-responsabili del trattamento (nel contratto, compreso un elenco di tali sub-responsabili in allegato), che dovrebbe essere integrata da criteri che guidino la scelta del responsabile del trattamento (ad esempio garanzie in termini di misure tecniche e organizzative, conoscenze specialistiche, affidabilità e risorse)[71]. In un contesto del genere, il responsabile del trattamento è tenuto a informare a tempo debito il titolare del trattamento in merito a eventuali aggiunte o sostituzioni previste di uno o più sub-responsabili del trattamento, in modo da garantire al titolare di cui sopra la possibilità di opporsi.

157. Pertanto, la differenza principale tra l'autorizzazione specifica e l'autorizzazione generale risiede nel significato attribuito al silenzio del titolare del trattamento: nel caso di un'autorizzazione generale, la mancata obiezione da parte del titolare del trattamento, entro il termine stabilito, può essere interpretata come assenso e quindi autorizzazione.

158. In entrambi i casi, il contratto dovrebbe prevedere informazioni dettagliate sulle tempistiche relative all'approvazione o meno da parte del titolare del trattamento e sulle modalità di comunicazione tra le parti a tal riguardo (ad esempio mediante modulistica specifica). Dette tempistiche devono essere ragionevoli in base al tipo di trattamento, alla complessità delle

attività affidate al responsabile (e ai sub-responsabili) del trattamento e al rapporto tra le parti. Inoltre, il contratto dovrebbe prevedere informazioni dettagliate sugli adempimenti concreti successivi a un'eventuale obiezione del titolare del trattamento (ad esempio specificando il termine entro cui il titolare e il responsabile dovrebbero pronunciarsi per porre fine al trattamento).

159. Indipendentemente dai criteri proposti dal titolare del trattamento nella scelta dei fornitori, il responsabile del trattamento conserva nei confronti del titolare l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile (articolo 28, paragrafo 4, del GDPR). Pertanto, il responsabile del trattamento si assicura di proporre sub-responsabili in grado di offrire garanzie sufficienti.

160. Inoltre, quando un responsabile del trattamento intende avvalersi di un sub-responsabile (autorizzato) deve concludere con quest'ultimo un contratto che preveda i medesimi obblighi imposti dal titolare al primo responsabile del trattamento; in alternativa, gli obblighi devono essere previsti da un altro atto giuridico, ai sensi del diritto dell'UE o dello Stato membro. L'intera catena delle attività di trattamento deve essere disciplinata da accordi scritti. L'imposizione dei «medesimi» obblighi dovrebbe essere interpretata in senso funzionale piuttosto che formale: non è necessario che il contratto contenga esattamente la stessa formulazione impiegata nel contratto tra il titolare e il responsabile del trattamento; tuttavia dovrebbe garantire che, nella sostanza, gli obblighi siano identici. Ciò significa anche che se il responsabile del trattamento affida a un sub-responsabile una parte specifica del trattamento, alla quale taluni obblighi non possono applicarsi, detti obblighi non dovrebbero essere inclusi «automaticamente» nel contratto con il sub-responsabile del trattamento in questione, in quanto ciò genererebbe solo incertezza. Ad esempio, per quanto concerne l'assistenza in materia di obblighi connessi a una violazione dei dati, la notifica di una tale violazione, da parte di un sub-responsabile del trattamento, direttamente al titolare potrebbe essere effettuata previo consenso di tutte e tre le parti. Tuttavia, nel caso di una notifica diretta, il responsabile del trattamento dovrebbe essere informato e ottenerne una copia.

2. CONSEGUENZE DELLA CONTITOLARITÀ DEL TRATTAMENTO

2.1 DETERMINAZIONE IN MODO TRASPARENTE DELLE RESPONSABILITÀ RISPETTIVE DEI CONTITOLARI DEL TRATTAMENTO PER QUANTO RIGUARDA IL RISPETTO DEGLI OBBLIGHI PREVISTI DAL GDPR

161. L'articolo 26, paragrafo 1, del GDPR stabilisce che i contitolari del trattamento determinano e concordano in modo trasparente le rispettive responsabilità in merito all'osservanza degli obblighi previsti dal regolamento.

162. I contitolari del trattamento stabiliscono pertanto «chi fa cosa» decidendo

tra loro chi dovrà svolgere un determinato compito, al fine di garantire la conformità agli obblighi applicabili, ai sensi del GDPR, in relazione al trattamento congiunto in questione. In altre parole, la ripartizione delle responsabilità in materia di conformità va effettuata in base all'uso del termine «*rispettive*» di cui all'articolo 26, paragrafo 1. Ciò non preclude il fatto che il diritto dell'UE o degli Stati membri possa già stabilire determinate responsabilità di ciascun contitolare del trattamento. In tal caso, l'accordo relativo al contitolare del trattamento dovrebbe contemplare altresì eventuali responsabilità aggiuntive, atte a garantire il rispetto del GDPR, non contemplate dalle disposizioni giuridiche[72].

163. L'obiettivo di tali norme è garantire che, laddove siano coinvolti più soggetti, in particolare in contesti di trattamento complessi, la responsabilità del rispetto delle norme in materia di protezione dei dati personali sia attribuita chiaramente, al fine di evitare che ne risulti sminuita o che un conflitto negativo di competenze dia luogo a lacune tali da consentire a una delle parti coinvolte nel trattamento di non rispettare taluni obblighi. Occorre chiarire che qualsivoglia responsabilità va attribuita in funzione delle circostanze di fatto, al fine di addivenire a un accordo operativo. L'EDPB osserva il verificarsi di situazioni ove l'influenza di un contitolare del trattamento e le relative conseguenze pratiche complicano il raggiungimento di un accordo. Tuttavia, tali circostanze non ostano alla contitolarità del trattamento e non possono esonerare le parti dai loro obblighi ai sensi del GDPR.

164. Più specificamente, l'articolo 26, paragrafo 1, prevede che la determinazione delle responsabilità rispettive (ossia dei compiti) ai fini dell'osservanza degli obblighi derivanti dal GDPR spetti ai contitolari del trattamento, «*con particolare riguardo*» all'esercizio dei diritti dell'interessato e alle rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le responsabilità rispettive dei titolari del trattamento siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.

165. Da tale disposizione emerge chiaramente che spetta ai contitolari del trattamento definire chi, rispettivamente, sarà incaricato di rispondere alle richieste laddove gli interessati esercitino i diritti loro conferiti dal GDPR e di fornire a questi ultimi le informazioni, a norma degli articoli 13 e 14 del GDPR. Si tratta soltanto di definire, nel loro rapporto interno, quali parti sono tenute a rispondere alle richieste degli interessati. Indipendentemente da tali accordi, l'interessato può contattare qualsivoglia contitolare del trattamento, a norma dell'articolo 26, paragrafo 3, del GPDR. Tuttavia, l'uso del termine «*con particolare riguardo*» significa che gli obblighi soggetti alla ripartizione delle responsabilità per la conformità di ciascuna delle parti interessate, di cui alla presente disposizione, non sono esaustivi. Ne consegue che, ai sensi del GDPR, la ripartizione delle responsabilità in materia di conformità tra i contitolari del trattamento non si limita agli aspetti di cui all'articolo 26, paragrafo 1, ma si estende ad altri obblighi di ciascun titolare. Di fatto, i contitolari del trattamento

sono tenuti a garantire che l'intero trattamento congiunto sia pienamente conforme al GDPR.

166. In quest'ottica, le misure di conformità e i relativi obblighi che i contitolari del trattamento dovrebbero prendere in considerazione, al momento di determinare le rispettive responsabilità, oltre a quelle specificamente menzionate all'articolo 26, paragrafo 1, riguardano tra l'altro, a titolo esemplificativo e in via non esaustiva,:

- l'attuazione dei principi generali di protezione dei dati (articolo 5);
- la base giuridica del trattamento[73] (articolo 6);
- le misure di sicurezza (articolo 32);
- la notifica di una violazione dei dati personali all'autorità di controllo e all'interessato[74] (articoli 33 e 34);
- le valutazioni d'impatto sulla protezione dei dati (articoli 35 e 36)[75];
- il ricorso a un responsabile del trattamento (articolo 28);
- i trasferimenti di dati verso paesi terzi (capo V);
- l'organizzazione del contatto con gli interessati e le autorità di controllo.

167. Altri temi che potrebbero essere presi in considerazione a seconda del trattamento in questione e dell'intenzione delle parti sono, ad esempio, le limitazioni all'uso dei dati personali per un'altra finalità da parte di uno dei contitolari del trattamento. A tale riguardo, i contitolari del trattamento sono sempre tenuti a garantire di disporre ciascuno di una base giuridica per il trattamento. Talvolta, nell'ambito della contitolarità del trattamento, i dati personali sono condivisi tra un titolare del trattamento e un altro. In termini di responsabilizzazione, ciascun titolare del trattamento ha il dovere di garantire che i dati non siano ulteriormente trattati in modo incompatibile con le finalità per le quali sono stati inizialmente raccolti dal titolare del trattamento che li condivide[76].

168. I contitolari del trattamento possono disporre di un certo grado di flessibilità nella distribuzione e nella ripartizione degli obblighi rispettivi, a condizione che garantiscano la piena conformità al GDPR per quanto concerne il trattamento in questione. Tale ripartizione dovrebbe tenere conto di fattori quali, ad esempio, chi è competente per e in grado di garantire efficacemente i diritti dell'interessato ovvero di rispettare gli obblighi pertinenti di cui al GDPR. L'EDPB raccomanda di documentare i fattori pertinenti e l'analisi interna effettuata al fine di ripartire i diversi obblighi. L'analisi fa parte della documentazione, in base al principio di responsabilizzazione.

169. Non è necessario che gli obblighi siano equamente distribuiti tra i contitolari del trattamento. A tale riguardo, la CGUE ha recentemente affermato che *«l'esistenza di una corresponsabilità non si traduce necessariamente in una responsabilità equivalente dei diversi operatori nell'ambito di un trattamento di dati personali»*[77]. Tuttavia, vi possono essere casi in cui non tutti gli obblighi possono essere ripartiti cosicché tutti i contitolari del trattamento possono essere tenuti ad adempiere agli stessi obblighi derivanti

dal GDPR, tenendo conto della natura e del contesto del trattamento congiunto. Ad esempio, i contitolari del trattamento che si avvalgono di strumenti o di sistemi condivisi di trattamento dei dati sono tenuti a garantire il rispetto, in particolare, del principio di limitazione delle finalità e ad attuare misure adeguate a garantire la sicurezza dei dati personali trattati nell'ambito di tali strumenti condivisi.

170. Un altro esempio è l'obbligo per ciascun contitolare del trattamento di tenere un registro delle attività di trattamento o di designare un responsabile della protezione dei dati (RPD) qualora siano soddisfatte le condizioni di cui all'articolo 37, paragrafo 1. Tali obblighi non sono legati al trattamento congiunto ma si applicano ai contitolari in quanto titolari del trattamento.

2.2 OBBLIGO DI EFFETTUARE LA RIPARTIZIONE DELLE RESPONSABILITÀ MEDIANTE UN ACCORDO

2.2.1 FORMA DELL'ACCORDO

171. L'articolo 26, paragrafo 1, del GDPR prevede come nuovo obbligo per i contitolari del trattamento di determinare le responsabilità rispettive «*mediante un accordo interno*». Il GDPR non specifica la forma giuridica di tale accordo. Pertanto, i contitolari del trattamento sono liberi di concordarne la forma.

172. Inoltre, l'accordo sulla ripartizione delle responsabilità è vincolante per ciascuno dei contitolari del trattamento. Ciascuno di essi concorda e si assume l'impegno *nei confronti degli altri* di essere responsabile dell'adempimento dei propri obblighi di cui all'accordo in quanto responsabilità propria.

173. Pertanto, ai fini della certezza del diritto, sebbene il GDPR non preveda requisiti giuridici relativi a un contratto o a un altro atto giuridico, l'EDPB raccomanda che tale accordo sia concluso sotto forma di documento vincolante, quale un contratto o un altro atto giuridico vincolante, ai sensi del diritto dell'UE o degli Stati membri cui i titolari del trattamento sono soggetti. Ciò garantirebbe certezza e potrebbe essere utilizzato per dimostrare il rispetto degli obblighi di trasparenza e responsabilizzazione. Di fatto, in caso di mancato rispetto della ripartizione concordata prevista dall'accordo, la natura vincolante di quest'ultimo consente a un titolare del trattamento di invocare la responsabilità dell'altro per quanto indicato nell'accordo come rientrante nella responsabilità di tale altro contitolare. Inoltre, in linea con il principio di responsabilizzazione, il ricorso a un contratto o altro atto giuridico consente ai contitolari del trattamento di dimostrare il rispetto degli obblighi imposti loro dal GDPR.

174. L'accordo dovrà esplicitare, in un linguaggio chiaro e semplice, il modo in cui le responsabilità, vale a dire i compiti, sono ripartiti tra ciascun contitolare del trattamento[78]. Tale requisito è importante in quanto garantisce

la certezza del diritto ed evita possibili conflitti non solo nei rapporti tra i contitolari del trattamento, ma anche nei confronti degli interessati e delle autorità di protezione dei dati.

175. Per inquadrare meglio la ripartizione delle responsabilità tra le parti, l'EDPB raccomanda che l'accordo contenga anche informazioni generali sul trattamento congiunto, specificando in particolare l'oggetto e la finalità di tale trattamento, le tipologie di dati personali e le categorie di interessati.

2.2.2 OBBLIGHI NEI CONFRONTI DEGLI INTERESSATI

176. Il GDPR prevede diversi obblighi dei contitolari del trattamento nei confronti degli interessati.

L'accordo deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari *nei confronti* degli interessati.

177. A integrazione di quanto illustrato nella sezione 2.1 delle presenti linee guida, è importante che i contitolari del trattamento chiariscano nell'accordo il ruolo rispettivo, *«con particolare riguardo»* all'esercizio dei diritti dell'interessato e alle funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14. L'articolo 26 del GDPR sottolinea l'importanza di tali obblighi specifici. I contitolari del trattamento devono pertanto prevedere e concordare come e da chi saranno fornite le informazioni nonché chi risponderà e in quale modo alle richieste dell'interessato. Indipendentemente dal contenuto dell'accordo su questo punto specifico, l'interessato può contattare uno dei contitolari del trattamento per esercitare i propri diritti, conformemente all'articolo 26, paragrafo 3, come spiegato di seguito.

178. La modalità di adempimento di tali obblighi come definita nell'accordo dovrebbe riflettere *«adeguatamente»*, ossia accuratamente, la realtà del trattamento congiunto. Ad esempio, se soltanto uno dei contitolari comunica con gli interessati ai fini del trattamento congiunto, tale contitolare potrebbe essere in una posizione migliore per informare gli interessati ed eventualmente rispondere alle loro richieste.

Obbligo di mettere a disposizione degli interessati gli elementi essenziali dell'accordo («Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato»)

179. Questa disposizione mira a garantire che l'interessato sia a conoscenza del *«contenuto essenziale dell'accordo»*. Ad esempio, deve essere del tutto chiaro all'interessato quale titolare del trattamento funga da punto di contatto per l'esercizio dei propri diritti (sebbene possa esercitare tali diritti nei confronti di e rispetto a qualsivoglia contitolare del trattamento). L'obbligo di mettere a disposizione degli interessati il contenuto essenziale dell'accordo è importante in caso di contitolarità del trattamento affinché l'interessato sappia chi tra i titolari del trattamento risponde di un determinato ambito.

180. Il GDPR non specifica quale sia il *«contenuto essenziale dell'accordo»*. L'EDPB raccomanda che tale contenuto essenziale riguardi almeno tutte le informazioni di cui agli articoli 13 e 14 che dovrebbero già essere accessibili all'interessato e, per ciascuno di tali elementi, l'accordo dovrebbe specificare il contitolare del trattamento responsabile di garantirne il rispetto. Il contenuto essenziale dell'accordo deve comprendere anche il punto di contatto, se designato.

181. Non viene specificato in che modo tali informazioni siano messe a disposizione dell'interessato. Contrariamente ad altre disposizioni del GDPR (quali l'articolo 30, paragrafo 4, in materia di registro dei trattamenti, o l'articolo 40, paragrafo 11, per il registro dei codici di condotta approvati), l'articolo 26 non prevede che la messa a disposizione debba essere *«su richiesta»* o *«resa pubblica mediante mezzi appropriati»*. Spetta pertanto ai contitolari del trattamento decidere il modo più efficace per mettere il contenuto essenziale dell'accordo a disposizione degli interessati (ad esempio allegandolo alle informazioni di cui all'articolo 13 o 14, inserendolo nella politica in materia di privacy o, su richiesta, comunicandolo al responsabile della protezione dei dati, se del caso, o al punto di contatto eventualmente designato). I contitolari del trattamento dovrebbero garantire, per quanto di rispettiva competenza, che le informazioni siano fornite in modo coerente.

Possibilità di designare nell'accordo un punto di contatto per gli interessati («Tale accordo può designare un punto di contatto per gli interessati»)

182. L'articolo 26, paragrafo 1, prevede la possibilità per i contitolari del trattamento di designare nell'accordo un punto di contatto per gli interessati. Detta designazione non è obbligatoria.

183. Il fatto di essere informati dell'esistenza di un singolo canale per contattare molteplici contitolari del trattamento consente agli interessati di sapere chi possono contattare in merito a tutte le questioni relative al trattamento dei loro dati personali. Inoltre, ciò consente ai contitolari del trattamento di coordinare in modo più efficiente i rapporti e le comunicazioni *nei confronti* degli interessati.

184. Per tali motivi, al fine di agevolare l'esercizio dei diritti degli interessati a norma del GDPR, l'EDPB raccomanda ai contitolari del trattamento di designare detto punto di contatto.

185. Il punto di contatto può essere l'eventuale responsabile della protezione dei dati, il rappresentante nell'Unione (per i contitolari del trattamento non stabiliti nell'Unione) o qualsivoglia altro punto di contatto presso il quale sia possibile ottenere informazioni.

Facoltà degli interessati di esercitare i propri diritti nei confronti di e contro ciascuno dei contitolari del trattamento, indipendentemente dai termini dell'accordo

186. Ai sensi dell'articolo 26, paragrafo 3, l'interessato non è vincolato dai termini dell'accordo e può esercitare i propri diritti ai sensi del GDPR nei con-

fronti di e contro ciascuno dei contitolari del trattamento.

187. Ad esempio, nel caso di contitolari del trattamento stabiliti in Stati membri diversi, o qualora solo uno dei contitolari sia stabilito nell'Unione, l'interessato può contattare, a sua scelta, il titolare del trattamento stabilito nello Stato membro in cui ha la residenza abituale o il luogo di lavoro oppure il titolare stabilito altrove nell'UE o nel SEE.

188. Anche se l'accordo e il relativo contenuto essenziale messo a disposizione degli interessati prevedono un punto di contatto per ricevere e trattare tutte le richieste degli interessati, questi ultimi possono comunque operare scelte diverse.

189. È pertanto importante che i contitolari del trattamento organizzino in anticipo la gestione delle risposte alle richieste che potrebbero ricevere dagli interessati. A tale riguardo, si raccomanda che i contitolari del trattamento comunichino agli altri titolari del trattamento responsabili o al punto di contatto designato le richieste da essi ricevute affinché siano trattate in modo efficace. Imporre agli interessati di contattare il punto di contatto designato o il titolare del trattamento competente costituirebbe un onere eccessivo, in contrasto con l'obiettivo di agevolare l'esercizio dei diritti degli interessati a norma del GDPR.

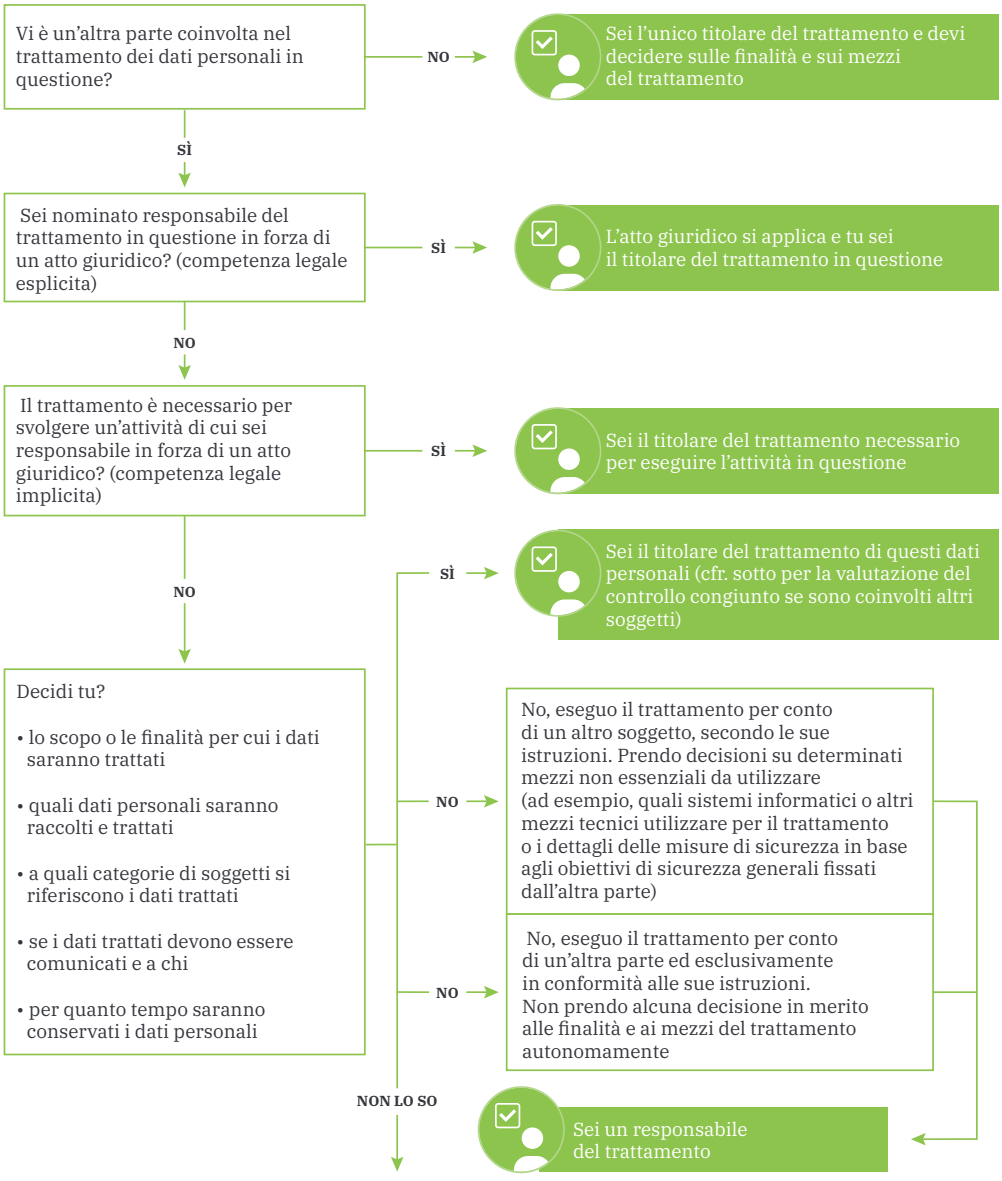
2.3 OBBLIGHI NEI CONFRONTI DELLE AUTORITÀ DI PROTEZIONE DEI DATI

190. I contitolari del trattamento dovrebbero prevedere nell'accordo le modalità di comunicazione con le autorità di controllo competenti. Le comunicazioni in questione potrebbero riguardare l'eventuale consultazione ai sensi dell'articolo 36 del GDPR, la notifica di una violazione dei dati personali e la designazione di un responsabile della protezione dei dati.

191. È opportuno rammentare che le autorità preposte alla protezione dei dati non sono vincolate dai termini dell'accordo per quanto concerne l'individuazione dei contitolari o del punto di contatto designato. Pertanto, in relazione al trattamento congiunto, le autorità possono contattare qualunque contitolare del trattamento per esercitare i loro poteri, a norma dell'articolo 58.

ALLEGATO I - DIAGRAMMA DI FLUSSO PER L'APPLICAZIONE PRATICA DEI CONCETTI DI TITOLARE DEL TRATTAMENTO, RESPONSABILE DEL TRATTAMENTO E CONTITOLARI DEL TRATTAMENTO

Nota: per valutare correttamente il ruolo di ciascuna entità conivolta, è necessario innanzitutto identificare il trattamento specifico dei dati personali in questione e l'esatta finalità. Se sono coinvolti più soggetti è necessario valutare se finalità e mezzi siano determinati congiuntamente, determinando una contitolarità del trattamento.



NON LO SO

Non so chi decide in merito alle finalità o ai mezzi del trattamento.

I seguenti fattori possono aiutare a determinare la qualificazione appropriata dei ruoli:

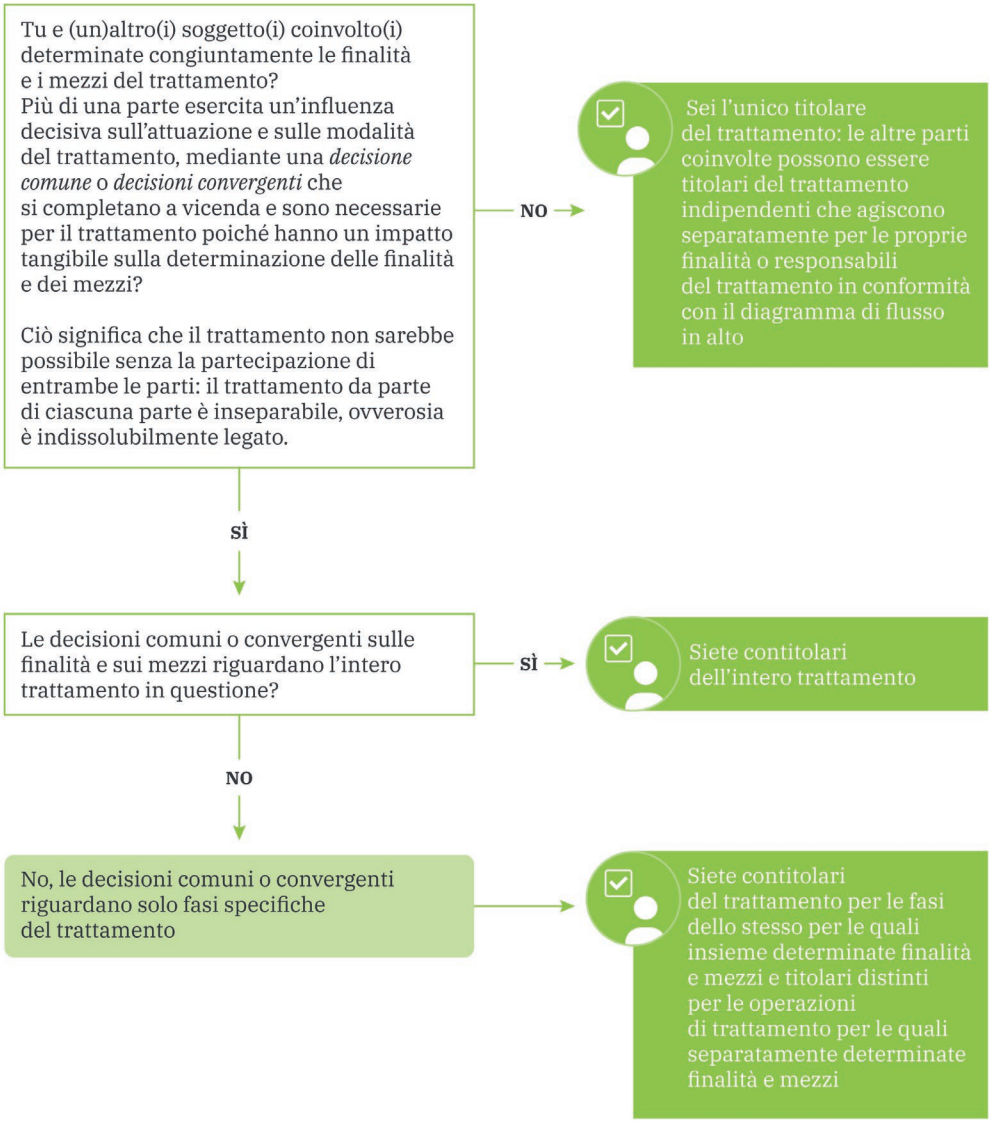
Fattori che indicano che sei il titolare del trattamento

- Trai un beneficio o hai un interesse nel trattamento (in misura diversa dal mero pagamento per i servizi ricevuti da un altro titolare del trattamento)
- Adotti decisioni sui soggetti interessati in quanto parte o risultato del trattamento (ad esempio, gli interessati sono i dipendenti)
- Le attività di trattamento possono considerarsi naturalmente collegate al ruolo o alle attività dell'entità di cui fai parte (ad esempio in ragione dei ruoli tradizionali o delle competenze professionali), il che comporta responsabilità dal punto di vista della protezione dei dati
- Il trattamento si riferisce al rapporto con gli interessati quali dipendenti, clienti, soci ecc.
- Hai completa autonomia nel decidere come sono trattati i dati personali
- Hai affidato il trattamento dei dati personali a un'organizzazione esterna per elaborare i dati personali per tuo conto

Fattori che indicano che sei il responsabile del trattamento

- Elabori i dati personali per le finalità di un'altra parte e in conformità con le sue istruzioni documentate; non hai una tua finalità propria per il trattamento.
- Un'altra parte monitora le tue attività di trattamento, al fine di garantire il rispetto delle istruzioni e dei termini del contratto.
- Non persegui finalità proprie nel trattamento se non il tuo interesse commerciale volto a fornire servizi.
- Sei stato incaricato di svolgere attività di trattamento specifiche da qualcuno che a sua volta è stato incaricato di trattare dati per conto di un'altra parte e su istruzioni documentate di questa parte (sei un sub - responsabile del trattamento)

CONTITOLARITÀ - SE SEI TITOLARE DEL TRATTAMENTO E ALTRE PARTI SONO COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI:



NOTE

[1] Nel presente documento, con «Stati membri» ci si riferisce agli «Stati membri del SEE».

[2] Gruppo di lavoro Articolo 29, Parere 1/2010 sui concetti di «responsabile del trattamento» e di «incaricato del trattamento», adottato il 16 febbraio 2010, 264/10/IT, WP 169.

[3] Gruppo di lavoro Articolo 29, Parere 3/2010 sul principio di responsabilizzazione, adottato il 13 luglio 2010, 00062/10/EN WP 173.

[4] Cfr. il considerando 74 del GDPR.

[5] Gruppo di lavoro Articolo 29, Parere 1/2010, WP 169, pag. 9.

[6] Cfr. anche le conclusioni dell'avvocato generale Mengozzi in *Testimoni di Geova*, C-25/17, ECLI:EU:C:2018:57, punto 68 («*ai fini della determinazione del "titolare del trattamento" ai sensi della direttiva 95/46, sono incline a ritenere [...] che un formalismo eccessivo renderebbe facile eludere le disposizioni della direttiva 95/46 e che, di conseguenza, occorre basarsi su un'analisi più fattuale che formale [...]*»).

[7] CGUE, causa C-131/12, Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, sentenza del 13 maggio 2014, punto 34; CGUE, causa C 210/16, Wirtschaftsakademie Schleswig-Holstein, sentenza del 5 giugno 2018, punto 28; CGUE, causa C 40/17, Fashion ID GmbH & Co.KG contro Verbraucherzentrale NRW eV, sentenza del 29 luglio 2019, punto 66.

[8] Ad esempio, nella sentenza relativa alla causa Testimoni di Geova, C-25/17, ECLI:EU:C:2018:551, punto 75, la CGUE ha ritenuto che una comunità religiosa di testimoni di Geova agisse come titolare del trattamento, insieme ai singoli membri. Sentenza nella causa Testimoni di Geova, C-25/17, ECLI:EU:C:2018:551, punto 75.

[9] In linea generale, ai sensi dell'articolo 29 del GDPR, i dipendenti aventi accesso ai dati personali all'interno di un'organizzazione non sono considerati «titolari del trattamento» o «responsabili del trattamento», bensì persone che «agiscono sotto l'autorità del titolare del trattamento o del responsabile del trattamento».

[10] Articolo 24, paragrafo 1, del GDPR.

[11] L'EDPB ritiene che questo esempio, precedentemente contemplato al considerando 47 della direttiva 95/46/CE, continui a essere pertinente anche ai sensi del GDPR.

[12] Cfr., ad esempio, gruppo di lavoro Articolo 29 per la protezione dei dati, Parere 10/2006 sul trattamento dei dati personali da parte della Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 novembre 2006, WP 128, pag. 11

[13] Cfr. parte I, sezione 3 («Definizione di contitolari del trattamento»).

[14] Cfr. anche le conclusioni dell'avvocato generale Bot nella causa *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2017:796, punto 46.

[15] Sentenza nella causa testimoni di Geova, C-25/17, ECLI:EU:C:2018:551, punto 68.

[16] Sentenza Fashion ID (C-40/17, ECLI:EU:C:2019:629, punto 74): «*Ne consegue, come rilevato, in sostanza, dall'avvocato generale [...] che una persona fisica o giuridica risulta poter essere responsabile, ai sensi dell'articolo 2, lettera d), della direttiva 95/46, insieme ad altri, soltanto delle operazioni di trattamento di dati personali di cui essa determina congiuntamente le finalità e gli strumenti. Per contro, [...] tale persona fisica o giuridica non può essere considerata responsabile, ai sensi di detta disposizione, delle operazioni anteriori o successive della catena di trattamento di cui essa non determina né le finalità né gli strumenti*».

[17] Sentenza nella causa *Wirtschaftsakademie*, C-201/16, ECLI:EU:c:2018:388, punto 38.

[18] Cfr., in particolare, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contro Wirtschaftsakademie,* (C-210/16), *Tietosuojavaltuutettu contro Jehovan todistajat – uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG contro Verbraucherzentrale NRW eV* (C-40/17). Va osservato che, sebbene tali sentenze siano state rese dalla CGUE sull'interpretazione del concetto di contitolari del trattamento ai sensi della direttiva 95/46/CE esse restano valide nell'ambito del GDPR, dato che gli elementi che determinano tale concetto, ai sensi del GDPR, rimangono invariati rispetto a quelli previsti dalla direttiva.

[19] In effetti, tutti gli accordi commerciali comportano la convergenza delle decisioni nell'ambito del processo mediante il quale viene raggiunto un accordo.

[20] Sentenza nella causa *Wirtschaftsakademie*, C-210/16, ECLI:EU:c:2018:388, punto 38.

[21] Sentenza nella causa *testimoni di Geova*, C-25/17, ECLI:EU-:C:2018:551, punto 75.

[22] Ibidem.

[23] Ibidem, punto 71.

[24] Ibidem.

[25] Sentenza nella causa Fashion ID, C-40/17, ECLI:EU:2018:1039, punto 74: *«Per contro, e fatta salva un'eventuale responsabilità civile prevista dal diritto nazionale a tal riguardo, tale persona fisica o giuridica non può essere considerata responsabile, ai sensi di detta disposizione, delle operazioni anteriori o successive della catena di trattamento di cui essa non determina né le finalità né gli strumenti».*

[26] Sentenza nella causa Fashion ID, C-40/17, ECLI:EU: 2018:1039, punto 80.

[27] Sentenza nella causa *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, punto 34.

[28] Sentenza nella causa *Wirtschaftsakademie*, C-210/16, ECLI :EU:C:2018:388, punto 39.

[29] Il fornitore del sistema può essere contitolare del trattamento se sono soddisfatti i criteri di cui sopra, ossia se partecipa alla determinazione delle finalità e dei mezzi. In caso contrario, il fornitore dovrebbe essere considerato responsabile del trattamento.

[30] Sentenza nella causa Fashion ID, C-40/17, ECLI:EU:2018:1039, punti 77-79.

[31] L'EDPB prevede di fornire ulteriori orientamenti in relazione alle sperimentazioni cliniche nel contesto delle prossime linee guida sul trattamento dei dati personali a fini medici e di ricerca scientifica.

[32] Cfr. parte I, sottosezione 2.1.4, sulla distinzione tra mezzi essenziali e non essenziali.

[33] Cfr. anche il considerando 81 del GDPR, che fa riferimento all'«affida[mento] delle attività di trattamento a un responsabile del trattamento», secondo cui le suddette attività, in quanto tali, sono una parte importante della decisione del titolare del trattamento di chiedere a un responsabile del trattamento di trattare dati personali per suo conto.

[34] Il datore di lavoro (in qualità di titolare del trattamento originario) potrebbe tuttavia continuare ad avere una certa responsabilità nel caso in cui il nuovo trattamento abbia luogo a causa della mancanza di misure di sicurezza adeguate.

[35] Cfr. anche il considerando 31 del GDPR.

[36] Ad esempio, il responsabile del trattamento dovrebbe assistere il titolare del trattamento, ove necessario e su richiesta, nel garantire l'adempimento degli obblighi relativi alle valutazioni d'impatto sulla protezione dei dati (considerando 95 del GDPR). Tale obbligo deve figurare nel contratto tra il titolare del trattamento e il responsabile del trattamento, ai sensi dell'articolo 28, paragrafo 3, lettera f), del GDPR.

[37] Articolo 28, paragrafo 1, e considerando 81 del GDPR.

[38] Cfr. il considerando 81 del GDPR.

[39] Articolo 28, paragrafo 5, e considerando 81 del GDPR.

[40] Cfr. anche l'articolo 28, paragrafo 3, lettera h), del GDPR.

[41] Articolo 28, paragrafo 9, del GDPR.

[42] La presenza (o l'assenza) di un accordo scritto, tuttavia, non è determinante ai fini della sussistenza di un rapporto titolare-responsabile del trattamento. Qualora, sulla base di un'analisi delle circostanze concrete relative al rapporto tra le parti e al trattamento dei dati personali in corso, vi sia motivo di ritenere che il contratto non corrisponda alla realtà in termini di controllo effettivo, si può non tenere conto di tale contratto. Di converso, un rapporto titolare-responsabile del trattamento potrebbe sussistere anche in assenza di un accordo di trattamento per iscritto. Ciò implicherebbe, tuttavia, una violazione dell'articolo 28, paragrafo 3, del GDPR. Inoltre, in determinate circostanze, l'assenza di una definizione chiara del rapporto tra il titolare e il responsabile del trattamento può comportare il problema della mancanza di una base giuridica su cui qualsivoglia trattamento dovrebbe basarsi, ad esempio in merito alla comunicazione dei dati tra il titolare e il presunto responsabile del trattamento.

[43] L'articolo 28, paragrafo 3, non si applica unicamente ai titolari del trattamento. Nel caso in cui solo il responsabile del trattamento sia soggetto all'ambito di applicazione territoriale di cui al GDPR, l'obbligo è direttamente applicabile unicamente a detto responsabile (cfr. anche le linee guida dell'EDPB 3/2018 sull'ambito di applicazione territoriale del RGPD, pag. 12).

[44] Articolo 28, paragrafo 6, del GDPR. L'EDPB rammenta che le clausole contrattuali tipo ai fini della conformità all'articolo 28 del GDPR non sono le stesse delle clausole contrattuali tipo di cui all'articolo 46, paragrafo 2. Mentre le prime precisano e chiariscono in che modo saranno soddisfatte le disposizioni di cui all'articolo 28, paragrafi 3 e 4, le seconde forniscono garanzie adeguate in caso di trasferimento di dati personali verso un paese terzo o verso un'organizzazione internazionale, in assenza

di una decisione di adeguatezza, ai sensi dell'articolo 45, paragrafo 3.

[45] Articolo 28, paragrafo 7, del GDPR; cfr. il parere congiunto 1/2021 dell'EDPB e del GEPD sulle clausole contrattuali tipo tra titolari e responsabili del trattamento https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_it.

[46] Articolo 28, paragrafo 8, del GDPR. Il registro delle decisioni adottate dalle autorità di controllo e dalle autorità giudiziarie su questioni trattate nell'ambito del meccanismo di coerenza, ivi comprese le clausole contrattuali tipo ai fini della conformità all'articolo 28 del GDPR, è disponibile al seguente indirizzo: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_it.

[47] Articolo 28, paragrafo 6, del GDPR.

[48] L'EDPB rammenta che, a norma dell'articolo 46, paragrafo 2, lettera c), o dell'articolo 46, paragrafo 2, lettera d) del GDPR, il medesimo grado di flessibilità è consentito quando le parti scelgono di avvalersi delle clausole contrattuali tipo come tutela adeguata per i trasferimenti verso paesi terzi. Il considerando 109 del GDPR chiarisce che «*la possibilità che il titolare del trattamento o il responsabile del trattamento utilizzi clausole tipo di protezione dei dati adottate dalla Commissione o da un'autorità di controllo non dovrebbe precludere ai titolari del trattamento o ai responsabili del trattamento la possibilità di includere tali clausole tipo in un contratto più ampio, anche in un contratto tra il responsabile del trattamento e un altro responsabile del trattamento, né di aggiungere altre clausole o garanzie supplementari, purché non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo [...] o ledano i diritti o le libertà fondamentali degli interessati. I titolari del trattamento e i responsabili del trattamento dovrebbero essere incoraggiati a fornire garanzie supplementari attraverso impegni contrattuali che integrino le clausole tipo di protezione*».

[49] Cfr. anche il parere 14/2019 dell'EDPB sul progetto di clausole contrattuali tipo presentato dall'autorità di controllo danese (articolo 28, paragrafo 8, del GDPR), pag. 5.

[50] Cfr. il considerando 79 del GDPR.

[51] Cfr. il considerando 81 del GDPR.

[52] La durata del trattamento non è necessariamente equivalente alla durata dell'accordo (possono sussistere obblighi giuridici di conservare i dati più a lungo o per un tempo inferiore).

[53] Cfr. parte II, sottosezione 1.5 («Responsabile del trattamento che determina le finalità e i mezzi del trattamento»).

[54] A tale riguardo, di converso, non è sufficiente, ad esempio, che il responsabile del trattamento si limiti a fornire al titolare del trattamento un accesso generalizzato a un elenco dei sub-responsabili del trattamento che potrebbe essere aggiornato, a cadenza periodica, senza comunicare i nominativi ogni nuovo sub-responsabile del trattamento previsto. In altre parole, il responsabile del trattamento deve informare attivamente il titolare del trattamento di qualsivoglia modifica dell'elenco (ovverosia, in particolare, di ogni nuovo sub-responsabile del trattamento previsto).

[55] Cfr. anche il parere 14/2019 dell'EDPB sul progetto di clausole contrattuali tipo presentato dall'autorità di controllo danese (articolo 28, paragrafo 8, del GDPR), del 9 luglio 2019, punto 44.

[56] Cfr. parte II, sottosezione 1.6 («Sub-responsabili»).

[57] Articolo 32 del GDPR.

[58] Articolo 33, paragrafo 3, del GDPR.

[59] Per maggiori informazioni, cfr. le Linee guida sulla notifica di violazioni dei dati personali ai sensi del regolamento (UE) 2016/679, WP 250 rev.01, 6 febbraio 2018, pagg. 13-14.

[60] Cfr. anche il parere 14/2019 dell'EDPB sul progetto di clausole contrattuali tipo presentato dall'autorità di controllo danese (articolo 28, paragrafo 8, del GDPR), del 9 luglio 2019, punto 40.

[61] Linee guida sulla notifica di violazioni dei dati personali ai sensi del regolamento (UE) 2016/679, WP 250 rev.01, 6 febbraio 2018, pag. 14.

[62] Gruppo di lavoro Articolo 29, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento «possa presentare un rischio elevato», ai fini del regolamento (UE) 2016/679, WP 248 rev.01, pag. 14.

[63] Cfr. il considerando 95 del GDPR.

[64] Cfr. parere congiunto 1/2021 dell'EDPB e del GEPD sulle clausole contrattuali tipo tra titolari e responsabili del trattamento, punto 43.

[65] Cfr. il parere 14/2019 sul progetto di clausole contrattuali tipo presentato dall'autorità di controllo danese (articolo 28, paragrafo 8, del GDPR), punto 43.

[66] Cfr. il parere 14/2019 sul progetto di clausole contrattuali tipo presentato dall'autorità di

controllo danese (articolo 28, paragrafo 8, del GDPR), punto 43.

[67] Cfr. parte II, sottosezione 1.6 («Sub-responsabili»).

[68] Cfr. parere congiunto 1/2021 dell'EDPB e del GEPD sulle clausole contrattuali tipo tra titolari e responsabili del trattamento, punto 39.

[69] Tali informazioni sono necessarie affinché il titolare del trattamento possa soddisfare il principio di responsabilità di cui all'articolo 24 e le disposizioni di cui all'articolo 28, paragrafo 1, all'articolo 32 e al capo V del GDPR.

[70] Cfr. parte II, sottosezione 1.1 («Scelta del responsabile del trattamento»).

[71] Tale dovere del titolare del trattamento deriva dal principio di responsabilità di cui all'articolo 24 e dall'obbligo di adempiere alle disposizioni di cui all'articolo 28, paragrafo 1, all'articolo 32 e al capo V del GDPR.

[72] «In ogni caso, l'accordo relativo al contitolare del trattamento dovrebbe contemplare in modo esaustivo tutte le responsabilità dei contitolari del trattamento, ivi comprese quelle che potrebbero già essere state definite nel diritto pertinente dell'UE o dello Stato membro e fatto salvo l'obbligo dei contitolari del trattamento di mettere a disposizione il contenuto essenziale dell'accordo che li riguarda, a norma dell'articolo 26, paragrafo 2, del GDPR».

[73] Sebbene il GDPR non impedisca ai contitolari del trattamento di avvalersi di una base giuridica diversa per i vari trattamenti da essi effettuati, si raccomanda di utilizzare, ove possibile, la stessa base giuridica per una finalità specifica.

[74] Cfr. altresì Gruppo di lavoro Articolo 29, Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 (WP 250.rev.01), a norma delle quali il controllo congiunto comprende la *«determinazione di chi sarà responsabile di adempiere agli obblighi di cui agli articoli 33 e 34. Il gruppo di lavoro Articolo 29 raccomanda che gli accordi contrattuali tra contitolari del trattamento prevedano disposizioni che stabiliscano quale titolare del trattamento assumerà il comando o sarà responsabile del rispetto degli obblighi di notifica delle violazioni previsti dal regolamento»* (pag. 14).

[75] Cfr. altresì le linee guida dell'EDPB sulle valutazioni d'impatto sulla protezione dei dati, WP 248.rev01, che stabiliscono quanto segue: *«Qualora il trattamento coinvolga contitolari del trattamento, questi ultimi devono definire con precisione le rispettive competenze. La loro valutazione d'impatto sulla protezione dei dati deve stabilire quale parte sia competente per le varie misure volte a trattare i rischi e a proteggere i diritti e le libertà degli interessati. Ciascun titolare del trattamento deve esprimere le proprie esigenze e condividere informazioni utili senza compromettere eventuali segreti (ad esempio protezione di segreti aziendali, proprietà intellettuale, informazioni aziendali riservate) o divulgare vulnerabilità.»* (pag. 8).

[76] Ogni comunicazione da parte di un titolare del trattamento richiede una base giuridica e una valutazione di compatibilità, indipendentemente dal fatto che il destinatario sia un diverso titolare del trattamento o un contitolare del trattamento. In altre parole, l'esistenza di un rapporto di contitolarità del trattamento non significa automaticamente che il contitolare che riceve i dati possa legittimamente trattarli anche per finalità aggiuntive che esulano dall'ambito della titolarità congiunta.

[77] Sentenza nella causa *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, punto 43.

[78] Come indicato al considerando 79 del GDPR, *«(...) la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità ai sensi del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento».*

Linee guida 8/2020 sul *targeting* degli utenti di social media Versione 2.0

Adottate il 13 aprile 2021

Cronologia delle versioni

Versione 2.0	13 aprile 2021	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	2 settembre 2020	Adozione delle linee guida ai fini della consultazione per la pubblicazione

Indice

1 Introduzione

2 Ambito di applicazione

3 Rischi per i diritti e le libertà degli utenti derivanti dal trattamento di dati personali

4 Soggetti coinvolti e ruoli
- 4.1 Utenti
- 4.2 Fornitori di social media
- 4.3 *Targeter*
- 4.4 Altri soggetti pertinenti
- 4.5 Ruoli e responsabilità

5 Analisi dei diversi meccanismi di *targeting*
- 5.1 Panoramica
- 5.2 *Targeting* sulla base di dati forniti
  - 5.2.1 Dati forniti dall'utente al fornitore di social media
    - A. Ruoli
    - B. Base giuridica
  - 5.2.2 Dati forniti al *targeter* dall'utente della piattaforma di social media
    - A. Ruoli
    - B. Base giuridica
- 5.3 *Targeting* sulla base di dati osservati
  - 5.3.1 Ruoli
  - 5.3.2 Base giuridica
- 5.4 *Targeting* sulla base di dati desunti
  - 5.4.1 Ruoli
  - 5.4.2 Base giuridica

6 Trasparenza e diritto di accesso
- 6.1 Contenuto essenziale dell'accordo e informazioni da fornire (articolo 26, paragrafo 2, GDPR)
- 6.2 Diritto di accesso (articolo 15)

7 Valutazioni d'impatto sulla protezione dei dati

8 Categorie particolari di dati
8.1 Che cosa costituisce una categoria particolare di dati
8.1.1 Appartenenza esplicita di un dato a una categoria particolare
8.1.2 Appartenenza di un dato a una categoria particolare sulla base di inferenze e combinazioni di informazioni
8.2 L'eccezione di cui all'articolo 9, paragrafo 2 per categorie particolari di dati resi manifestamente pubblici

9 Contitolarità e responsabilità congiunta
9.1 Accordo tra i contitolari del trattamento e determinazione delle responsabilità (articolo 26 GDPR)
9.2 Livelli di responsabilità

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati),

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

1. INTRODUZIONE

1. Uno sviluppo significativo registrato nel contesto online nell'ultimo decennio è stato dato dall'ascesa dei social media. Sempre più persone utilizzano i social media per rimanere in contatto con familiari ed amici, per sviluppare reti professionali o per creare collegamenti in relazione a interessi e idee condivisi. Ai fini delle presenti linee guida, con "social media" si intendono piattaforme online che consentono lo sviluppo di reti e di comunità di utenti, tra i quali vengono condivisi contenuti e informazioni[1]. Tra le caratteristiche principali dei social media figurano la possibilità per le persone fisiche di registrarsi al fine di creare "account" (conti) o "profili" per sé stesse, di interagire tra loro condividendo contenuti generati dagli utenti o altri contenuti nonché di sviluppare collegamenti e reti con altri utenti[2].

2. Nell'ambito del loro modello aziendale numerosi fornitori di social media offrono servizi di *targeting*. I servizi di *targeting* consentono a persone fisiche o giuridiche ("*targeter*") di comunicare messaggi specifici agli utenti di social media per promuovere interessi commerciali, politici o di altro tipo[3]. Una caratteristica distintiva del *targeting* è l'adeguatezza percepita tra la persona o il gruppo a cui ci si rivolge e il messaggio che viene trasmesso. Secondo l'assunto alla base di tale attività, migliore è l'adeguatezza del messaggio, maggiore è il tasso di ricezione (conversione) e quindi più efficace è la campagna di *targeting* (utile sul capitale investito).

3. La sofisticazione dei meccanismi per rivolgersi in maniera mirata agli utenti di social media è aumentata nel tempo. Le organizzazioni dispongono attualmente della possibilità di rivolgersi in maniera mirata alle persone fisiche sulla base di una vasta gamma di criteri. Tali criteri possono essere stati sviluppati sulla scorta di dati personali che gli utenti hanno attivamente fornito o condiviso, quali il loro stato di relazione. Sempre più spesso, tuttavia, i criteri del *targeting* sono sviluppati anche sulla base di dati personali osservati o desunti, tanto dal fornitore di social media quanto da terzi, e raccolti (aggregati) dalla piattaforma o da altri soggetti (ad esempio gli intermediari di dati) per sostenere le opzioni di *targeting* pubblicitario. In altri termini, il *targeting* degli utenti di social media non implica soltanto l'atto di "selezionare" le persone fisiche o i gruppi di persone fisiche che sono i destinatari previsti di un determinato messaggio (la "platea di destinatari"), quanto piuttosto un intero processo svolto da un insieme di soggetti che si traduce nella veicolazione di messaggi specifici alle persone fisiche che dispongono di account sui social media[4].

4. La combinazione e l'analisi dei dati provenienti da fonti diverse, associate alla natura potenzialmente sensibile dei dati personali trattati nel contesto dei social media[5], genera rischi in termini di diritti e libertà fondamentali delle persone fisiche. Dal punto di vista della protezione dei dati, numerosi rischi riguardano la possibile mancanza di trasparenza e di controllo da parte dell'utente. Per le persone fisiche interessate, il trattamento sottostante dei dati personali che si traduce nella veicolazione di un messaggio mirato è spesso opaco. Inoltre può comportare usi imprevisti o indesiderati dei dati

personali, che sollevano questioni non soltanto in termini di normativa sulla protezione dei dati, ma anche in relazione ad altri diritti e ad altre libertà fondamentali. Di recente il *targeting* sui social media ha attirato un maggiore interesse da parte del pubblico ed è stato soggetto a un esame normativo nel contesto del processo decisionale democratico e dei processi elettorali[6].

2. AMBITO DI APPLICAZIONE

5. Il *targeting* degli utenti di social media può coinvolgere una varietà di soggetti diversi che, ai fini delle presenti linee guida, saranno suddivisi in quattro gruppi: i fornitori di social media, i loro utenti, i *targeter* ed altri soggetti che possono essere coinvolti nel processo di *targeting*. L'importanza di individuare correttamente i ruoli e le responsabilità dei vari soggetti è stata recentemente messa in evidenza dalle sentenze della Corte di giustizia dell'Unione europea (in appresso, la Corte) nelle cause *Wirtschaftsakademie* e *Fashion ID*[7]. Entrambe le sentenze dimostrano che l'interazione tra i fornitori di social media e altri soggetti può dar luogo a responsabilità congiunte ai sensi del diritto dell'UE in materia di protezione dei dati.
6. Tenendo conto della giurisprudenza della Corte, nonché delle disposizioni del GDPR in materia di contitolari del trattamento e di responsabilizzazione, le presenti linee guida offrono orientamenti in merito al *targeting* degli utenti di social media, in particolare per quanto concerne le responsabilità dei *targeter* e dei fornitori di social media. Laddove esista una responsabilità congiunta, le linee guida cercheranno di chiarire quale potrebbe essere la distribuzione delle responsabilità tra i *targeter* e i fornitori di social media sulla base di esempi pratici.
7. Le presenti linee guida mirano pertanto in via primaria a chiarire i ruoli e le responsabilità tra il fornitore di social media e il *targeter*. A tal fine, le linee guida individuano anche i rischi potenziali per i diritti e le libertà delle persone fisiche (sezione 3), i soggetti principali e i loro ruoli (sezione 4) ed esaminano l'applicazione dei requisiti principali della protezione dei dati (quali liceità e trasparenza, valutazione d'impatto sulla protezione dei dati, ecc.) nonché gli elementi chiave degli accordi tra fornitori di social media e *targeter*.
8. Ciò nonostante, l'ambito delle presenti linee guida include le relazioni tra gli utenti registrati di una rete sociale, i fornitori di quest'ultima, nonché i . Un'analisi approfondita delle diverse situazioni, per esempio relativamente alle persone fisiche che non sono registrate con fornitori di social media, esula dall'ambito delle presenti linee guida[8].

3. RISCHI PER I DIRITTI E LE LIBERTÀ DEGLI UTENTI DERIVANTI DAL TRATTAMENTO DI DATI PERSONALI

9. Il GDPR sottolinea l'importanza di valutare adeguatamente e attenuare qual-

siasi rischio per i diritti e le libertà delle persone fisiche derivante dal trattamento di dati personali.[9] I meccanismi utilizzabili per rivolgersi in maniera mirata agli utenti di social media, così come le attività di trattamento sottostanti che consentono il *targeting*, possono comportare rischi significativi. Le presenti linee guida non intendono fornire un elenco esaustivo dei rischi per i diritti e le libertà delle persone fisiche. Ciò nonostante l'EDPB ritiene importante segnalare alcuni tipi di rischi e fornire una serie di esempi in merito alle modalità con cui possono manifestarsi.

10. Il *targeting* degli utenti di social media può comportare un uso dei dati personali che va contro oppure oltre le ragionevoli aspettative delle persone fisiche e quindi viola i principi e le norme applicabili in materia di protezione dei dati. Ad esempio, quando una piattaforma di social media associa i dati personali provenienti da fonti terze ai dati divulgati dagli utenti della piattaforma stessa, ciò può comportare un utilizzo dei dati personali ulteriore rispetto alla finalità iniziale e secondo modalità che la persona fisica non poteva ragionevolmente prevedere. Le attività di profilazione collegate al *targeting* potrebbero comportare un'inferenza di interessi o altre caratteristiche, che la persona fisica non aveva attivamente rivelato, minando così la capacità di quest'ultima di esercitare il controllo sui suoi dati personali[10]. Inoltre una mancanza di trasparenza sul ruolo dei diversi soggetti e sui trattamenti coinvolti può compromettere, complicare od ostacolare l'esercizio dei diritti degli interessati.

11. Un secondo ambito di rischio riguarda la possibilità di discriminazione ed esclusione. Il *targeting* degli utenti di social media può comportare criteri che, direttamente o indirettamente, hanno effetti discriminatori in relazione all'origine razziale o etnica di una persona fisica, al suo stato di salute o al suo orientamento sessuale o ad altre caratteristiche protette della persona fisica in questione. Ad esempio l'uso di tali criteri nel contesto della pubblicità relativa a offerte di lavoro, di alloggi o di linee di credito (prestiti, mutui) può ridurre la visibilità delle opportunità da parte delle persone appartenenti a determinati gruppi. Il potenziale di discriminazione insito nel *targeting* deriva dalla capacità degli inserzionisti di sfruttare l'ampia quantità e varietà di dati personali (ad esempio dati demografici, comportamentali e sugli interessi) che le piattaforme di social media raccolgono sui loro utenti[11]. Ricerche recenti suggeriscono che il rischio di effetti discriminatori esiste anche senza utilizzare criteri che sono direttamente legati a categorie particolari di dati personali di cui all'articolo 9 del GDPR[12].

12. Una terza categoria di rischio riguarda la possibile manipolazione degli utenti. Per definizione, i meccanismi di *targeting* sono utilizzati per influenzare il comportamento e le scelte delle persone fisiche, tanto in relazione alle loro decisioni di acquisto in veste di consumatori quanto in termini di loro decisioni politiche in qualità di cittadini impegnati nella vita civile[12]. Alcuni approcci di *targeting* possono tuttavia arrivare al punto di minare l'autonomia e la libertà individuali (ad esempio, inviando messaggi personalizzati concepiti per sfruttare o addirittura accentuare alcune vulnerabilità, alcuni valori personali o alcune preoccupazioni). Un'analisi dei contenuti condivisi

attraverso i social media può rivelare informazioni sullo stato emotivo (ad esempio, attraverso l'analisi dell'impiego di determinate parole chiave). Tali informazioni potrebbero essere utilizzate per rivolgere alla persona fisica messaggi mirati specifici e in momenti specifici nei quali ci si aspetta che sia più ricettiva, influenzando così surrettiziamente il suo processo di pensiero, le sue emozioni e il suo comportamento[14].

13. I meccanismi per rivolgersi in maniera mirata agli utenti di social media possono essere sfruttati altresì per influenzare indebitamente le persone fisiche nel contesto del confronto politico e dei processi elettorali democratici[15]. Mentre le campagne politiche "tradizionali" offline mirano a influenzare il comportamento degli elettori attraverso messaggi che sono generalmente disponibili e recuperabili (verificabili), i meccanismi di *targeting* online disponibili consentono ai partiti politici e alle campagne politiche di rivolgersi ai singoli elettori con messaggi personalizzati specifici per le esigenze, gli interessi e i valori della platea di destinatari[16]. Tale attività di *targeting* potrebbe comportare altresì disinformazione o la veicolazione di messaggi che suscitano particolare disagio nelle persone, e riescono quindi (più facilmente) a suscitare una determinata emozione o reazione da parte loro. Quando messaggi polarizzanti o non veritieri (disinformazione) sono rivolti a persone fisiche specifiche, senza contestualizzazione o esposizione ad altri punti di vista oppure con una limitata contestualizzazione ed esposizione a tali altri punti di vista, l'uso di meccanismi di *targeting* può avere l'effetto di minare il processo elettorale democratico[17].

14. Analogamente, l'uso di algoritmi per determinare quali informazioni mostrare alle diverse persone può influenzare negativamente la probabilità di accesso a fonti diversificate di informazioni in relazione a un particolare argomento. A sua volta ciò può avere conseguenze negative per il pluralismo del dibattito pubblico e l'accesso all'informazione[18]. I meccanismi di *targeting* possono essere utilizzati per aumentare la visibilità di determinati messaggi, dando meno risalto ad altri. Il potenziale impatto negativo può avere ripercussioni su due livelli. Da un lato, vi sono rischi legati alle cosiddette "bolle di filtraggio" (*filter bubbles*) che si verificano quando le persone sono esposte a "più informazioni dello stesso tipo" e si confrontano con un numero minore di punti di vista, il che aumenta la polarizzazione politica e ideologica[19]. Dall'altro, i meccanismi di *targeting* possono generare rischi di "sovraccarico informativo", cosicché le persone non sono in grado di prendere una decisione informata perché dispongono di troppe informazioni e non riescono a stabilire se siano affidabili.

15. La raccolta di dati personali da parte dei fornitori di social media può non essere limitata alle attività svolte dalle persone fisiche sulla piattaforma stessa di social media. Il *targeting* degli utenti di social media sulla base di informazioni riguardanti il loro comportamento di navigazione o altre attività al di fuori della piattaforma di social media può dare alle persone la sensazione che il loro comportamento sia monitorato sistematicamente. Ciò può avere un effetto paralizzante sulla libertà di espressione, compreso l'accesso all'informazione[20]. Tali effetti possono essere esacerbati se il *targeting* si

basa anche sull'analisi dei contenuti condivisi dagli utenti di social media. Se i messaggi privati, i post e i commenti sono soggetti ad analisi per un uso commerciale o politico, ciò può altresì dare origine a forme di autocensura.

16. Il potenziale impatto negativo del *targeting* può essere considerevolmente maggiore quando sono coinvolte categorie vulnerabili di persone fisiche, come i minori. Il *targeting* può influenzare la formazione delle preferenze e degli interessi personali dei minori, incidendo in definitiva sulla loro autonomia e sul loro diritto allo sviluppo. Il considerando 38 GDPR afferma che tale specifica protezione dovrebbe riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore[21].

17. L'impiego dei social media nell'UE è diffuso, dato che il 54 % delle persone tra i 16 e i 74 anni ha partecipato ai social network nel 2019. Inoltre tale tasso di partecipazione è aumentato costantemente nel corso degli anni[22]. L'EDPB riconosce che l'aumento della concentrazione nei mercati dei social media e del *targeting* può aumentare altresì i rischi per i diritti e le libertà di un numero sostanziale di persone fisiche. Ad esempio alcuni fornitori di social media possono essere in grado di combinare, da soli o in connessione con altre imprese, una quantità e varietà maggiori di dati personali. A sua volta, ciò può aumentare la capacità di offrire campagne di *targeting* più avanzate. Questo aspetto è rilevante tanto dal punto di vista della protezione dei dati (profilazione più approfondita delle persone interessate) quanto dal punto di vista del diritto in materia di concorrenza (le ineguagliabili capacità di approfondimento fornite dalla piattaforma possono renderla un "partner commerciale inevitabile" per gli operatori online). Il grado di potere di mercato e informativo, a sua volta, come riconosciuto dall'EDPB, "*rischia di incidere sul livello di protezione dei dati e delle libertà di cui godono i consumatori di servizi digitali*"[23].

18. La probabilità e la gravità dei rischi summenzionati dipenderanno, tra l'altro, dalla natura del meccanismo di *targeting* nonché dalle modalità e dalle finalità precise per le quali viene utilizzato. Gli elementi che possono influenzare la probabilità e la gravità dei rischi nel contesto del *targeting* degli utenti di social media saranno discussi più in dettaglio nella sezione 7.

4. SOGGETTI COINVOLTI E RUOLI

4.1 UTENTI

19. Le persone fisiche fanno uso dei social media a diverso titolo e per diverse finalità (ad esempio per rimanere in contatto con gli amici, per scambiare informazioni su interessi comuni o per cercare opportunità di lavoro). Il termine "utente" è utilizzato di norma per riferirsi a persone fisiche che si sono registrate al servizio (ossia quelle che dispongono di un "account" o un "profilo"). Numerosi servizi di social media possono tuttavia essere accessibili

anche a persone fisiche in assenza di registrazione (ossia senza la necessità di creare un account o un profilo)[24]. In genere tali persone fisiche non sono in grado di fare uso di tutte le funzionalità o di tutti i servizi offerti a chi si è registrato presso il fornitore di social media. Tanto le persone fisiche registrate quanto quelle che non sono registrate presso i fornitori di social media possono essere considerate "interessati" ai sensi dell'articolo 4, punto 1, GDPR nella misura in cui la persona fisica è direttamente o indirettamente identificata o identificabile[25].

20. Le persone fisiche possono registrarsi utilizzando un nome reale, oppure un soprannome (*nickname*) o uno pseudonimo, a seconda delle politiche adottate dallo specifico servizio di social media. In genere sarà comunque possibile rivolgersi in maniera mirata (o altrimenti individuare) l'utente in questione anche in assenza di una politica che richieda l'utilizzo del nome reale, in quanto la maggior parte dei *targeting* non si basa sui nomi degli utenti quanto piuttosto su altri tipi di dati personali quali gli interessi, i dati sociografici, il comportamento o altri identificatori. I fornitori di social media incoraggiano spesso i loro utenti a rivelare dati del "mondo reale" quali i numeri di telefono[26]. Infine vale la pena osservare che i fornitori di social media possono altresì consentire il *targeting* di persone fisiche che non hanno un account con tali fornitori[27].

4.2 FORNITORI DI SOCIAL MEDIA

21. I fornitori di social media offrono un servizio online che consente lo sviluppo di reti e comunità di utenti, tra i quali vengono condivise informazioni e contenuti. I servizi di social media sono in genere offerti attraverso browser web o app dedicate, spesso dopo aver richiesto all'utente di fornire una serie di dati personali per costituire il suo "account" o "profilo". Spesso offrono agli utenti anche dei "controlli" associati all'account per consentire loro di accedere e controllare i dati personali trattati nel contesto dell'uso del loro account.

22. Il fornitore di social media determina le funzionalità del servizio. Ciò a sua volta implica una determinazione di quali dati vengono trattati, per quale finalità, in quali termini, così come le modalità di trattamento dei dati personali. Ciò consente la fornitura del servizio di social media ma anche probabilmente la fornitura di servizi, quali il *targeting*, che possono apportare vantaggi ai partner commerciali che operano sulla piattaforma di social media o in combinazione con essa.

23. Il fornitore di social media ha la possibilità di raccogliere grandi quantitativi di dati personali relativi al comportamento e alle interazioni di utenti e persone fisiche che non sono registrati presso i fornitori di social media, circostanza questa che gli consente di ottenere notevoli approfondimenti in merito alle caratteristiche socio-demografiche, agli interessi e alle preferenze degli utenti. È importante notare che gli "approfondimenti" basati sull'attività degli utenti spesso coinvolgono dati personali desunti o deriva-

ti. Ad esempio quando un utente interagisce con un determinato contenuto (lasciando un "mi piace" su un post sui social media oppure guardando un contenuto video), tale azione può essere registrata dal fornitore di social media che può desumere che l'utente in questione ha apprezzato il contenuto con cui ha interagito.

24. I fornitori di social media raccolgono sempre più dati non soltanto dalle attività sulla piattaforma stessa, ma anche dalle attività intraprese "al di fuori dalla piattaforma", combinando dati provenienti da più fonti, online e offline, al fine di generare ulteriori approfondimenti. I dati possono essere associati ai dati personali che le persone fisiche rivelano attivamente al fornitore di social media (ad esempio, un nome utente, un indirizzo di posta elettronica, un'ubicazione e un numero di telefono), così come ai dati che vengono "assegnati" loro dalla piattaforma (quali gli identificatori univoci).

4.3 *TARGETER*

25. Le presenti linee guida utilizzano il termine *targeter* per designare le persone fisiche o giuridiche che utilizzano i servizi di social media per indirizzare messaggi specifici a un insieme di utenti di social media sulla base di parametri o criteri specifici[28]. Ciò che distingue i *targeter* dagli altri utenti di social media è il fatto che selezionano i loro messaggi e/o la platea di destinatari in base alle caratteristiche, agli interessi o alle preferenze percepiti delle persone fisiche in questione, una pratica che a volte viene denominata anche "*micro-targeting*"[29]. I *targeter* possono svolgere attività di *targeting* per promuovere interessi commerciali, politici o di altro tipo. Esempi tipici sono i marchi che sfruttano i social media per pubblicizzare i loro prodotti, nonché per aumentare la consapevolezza del marchio. Anche i partiti politici stanno facendo sempre più uso dei social media come parte della loro strategia di campagna. Anche gli enti di beneficenza e altre organizzazioni senza scopo di lucro utilizzano i social media per rivolgere messaggi mirati a potenziali finanziatori o per sviluppare comunità.

26. È importante osservare che ci si può rivolgere in maniera mirata agli utenti di social media in modi diversi. Ad esempio, il *targeting* potrebbe avvenire non soltanto attraverso la visualizzazione di pubblicità personalizzata (attraverso un "banner" visualizzato nella parte superiore o laterale di una pagina web) ma, nella misura in cui avviene all'interno della piattaforma di social media, anche attraverso la visualizzazione nel "feed", nel "diario" o nella "storia" di un utente, dove il contenuto pubblicitario appare accanto al contenuto generato dall'utente. Il *targeting* può inoltre comportare la creazione di contenuti ospitati dal fornitore di social media (per esempio tramite una "pagina" dedicata o un'altra presenza sui social media) oppure altrove (per esempio su siti web di terzi). I *targeter* possono avere siti web e applicazioni propri, dove possono integrare strumenti specifici aziendali dei social media o funzionalità quali i plug-in o i login sociali oppure utilizzando le interfacce di programmazione delle applicazioni (API) o i kit di sviluppo del software (SDK) offerti dai fornitori di social media.

4.4 ALTRI SOGGETTI PERTINENTI

27. I *targeter* possono utilizzare direttamente i meccanismi di *targeting* offerti da fornitori di social media oppure integrare servizi di altri soggetti, quali i fornitori di servizi di marketing, le reti pubblicitarie, gli scambiatori di pubblicità, piattaforme sul lato della domanda e dell'offerta (piattaforme per la vendita e l'acquisto automatizzati di spazi pubblicitari, ndt), i fornitori di gestione dei dati e le imprese di analisi dei dati (*data analytics*). Tali soggetti fanno parte del complesso ecosistema in evoluzione della pubblicità online (a volte denominato anche "*adtech*") che raccoglie e tratta i dati relativi alle persone fisiche (compresi gli utenti di social media) ad esempio tracciando le loro attività su siti web e applicazioni[30].

28. Anche gli intermediari di dati e i fornitori di gestione dei dati sono soggetti pertinenti che svolgono un ruolo importante nel *targeting* degli utenti di social media. Gli intermediari di dati e i fornitori di gestione dei dati si differenziano dalle altre imprese *adtech* nella misura in cui non trattano soltanto i dati raccolti per mezzo di tecnologie di tracciamento, ma anche dati raccolti da altre fonti, che possono essere tanto online quanto offline. In altre parole, gli intermediari di dati e i fornitori di gestione dei dati aggregano i dati raccolti da un'ampia varietà di fonti, che poi possono vendere ad altre parti interessate coinvolte nel processo di *targeting*.

29. Sebbene ciascuno degli altri soggetti sopra menzionati possa svolgere un ruolo importante nel *targeting* degli utenti di social media, l'attenzione delle presenti linee guida è incentrata sulla distribuzione dei ruoli e degli obblighi di protezione dei dati rispetto ai fornitori di social media e ai *targeter*. Considerazioni analoghe possono applicarsi tuttavia agli altri soggetti facenti parte dell'ecosistema della pubblicità online, a seconda del ruolo svolto da ciascuno di essi nel processo di *targeting*[31].

4.5 RUOLI E RESPONSABILITÀ

30. Al fine di chiarire i ruoli e le responsabilità rispettivi dei fornitori di social media e dei *targeter*, è importante prendere in considerazione la giurisprudenza pertinente della Corte. Le sentenze nelle cause *Wirtschaftsakademie* (C-210/16), *Jehovah's Witnesses* (C25/17) e *Fashion ID* (C-40/17) sono particolarmente pertinenti in questo caso.

31. Il punto di partenza dell'analisi è la definizione giuridica di titolare del trattamento. Secondo l'articolo 4, punto 7, GDPR, per "titolare del trattamento" si intende "*la persona fisica o giuridica [...] che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*".

32. Nella causa *Wirtschaftsakademie*, la Corte ha deciso che l'amministratore di una cosiddetta "fanpage" presente su Facebook partecipa alla determinazione delle finalità e degli strumenti del trattamento dei dati personali. Secondo le osservazioni formulate dalla Corte, la creazione di una fanpage comporta l'impostazione di parametri da parte dell'amministratore, che *influisce* sul

trattamento di dati personali ai fini della creazione di statistiche stabilite a partire dalle visite della fanpage[32]. Utilizzando i filtri forniti da Facebook, l'amministratore può definire i criteri secondo i quali devono essere elaborate le statistiche nonché designare le categorie di persone i cui dati personali devono essere utilizzati da Facebook:

"In particolare, l'amministratore della fanpage può chiedere di ricevere – e, quindi, chiedere che siano trattati – dati demografici concernenti il suo pubblico destinatario, in particolare tendenze in materia di età, sesso, situazione sentimentale e professionale, informazioni sullo stile di vita e sugli interessi di detto pubblico, nonché informazioni sugli acquisti e il comportamento di acquisto online dei visitatori della sua pagina, le categorie di prodotti o di servizi di loro maggiore interesse, come pure dati territoriali che consentono all'amministratore della fanpage di stabilire dove avviare promozioni speciali o organizzare eventi e, in generale, di offrire informazioni maggiormente mirate".

33. Poiché la definizione dei parametri dipende tra l'altro dal pubblico di riferimento dell'amministratore "e dagli obiettivi di gestione e promozione delle sue attività", l'amministratore partecipa anche alla determinazione delle finalità del trattamento dei dati personali[33]. L'amministratore è stato quindi ritenuto un titolare del trattamento, responsabile del trattamento dei dati personali dei visitatori della sua "pagina" congiuntamente al fornitore del social media.

34. Come ulteriormente sviluppato nella sezione 9 delle presenti linee guida, i titolari del trattamento possono essere coinvolti in fasi diverse del trattamento di dati personali e a diversi livelli. In tali circostanze, il livello di responsabilità di ciascuno di essi deve essere valutato in relazione a tutte le circostanze rilevanti del caso specifico:

"l'esistenza di una responsabilità congiunta non implica necessariamente una responsabilità equivalente, per un medesimo trattamento di dati personali, dei diversi soggetti che vi partecipano. Al contrario, tali soggetti possono essere coinvolti in fasi diverse di tale trattamento e a diversi livelli, di modo che il grado di responsabilità di ciascuno di essi deve essere valutato tenendo conto di tutte le circostanze rilevanti del caso di specie"[34].

35. Pur concludendo che l'amministratore di una pagina agisce in veste di titolare del trattamento, congiuntamente a Facebook, la Corte ha osservato altresì che nel caso in questione, Facebook deve essere considerato come il soggetto che determina, *in via preliminare*, le finalità e gli strumenti del trattamento dei dati personali degli utenti di Facebook nonché delle persone che visitano la fanpage presente su Facebook[35].

36. Nella sentenza *Fashion ID*, la Corte ha deciso che il gestore di un sito internet può essere considerato un titolare del trattamento quando inserisce un plug-in sociale di Facebook sul proprio sito internet che consente al browser del visitatore di trasferire dati personali del visitatore a Facebook[36]. La qualifica del gestore del sito internet come titolare del trattamento è tuttavia limitata all'operazione o all'insieme di operazioni di relazione alla/al quale determina effettivamente le finalità e i mezzi. In questo caso specifico, la Corte ha con-

siderato che il gestore del sito internet è in grado di determinare, insieme a Facebook, soltanto le finalità e i mezzi della raccolta e della divulgazione per trasmissione dei dati personali dei visitatori del proprio sito. Di conseguenza la Corte ha stabilito che, per quanto riguarda l'incorporazione di un plug-in sociale all'interno di un sito web, la responsabilità del gestore del sito è:

"limitata all'operazione o all'insieme delle operazioni di trattamento dei dati personali di cui determina effettivamente le finalità e gli strumenti, vale a dire la raccolta e la comunicazione mediante trasmissione dei dati di cui trattasi"[37].

37. La Corte ha ritenuto che il gestore del sito internet non fosse un titolare del trattamento per le successive operazioni[38] di trattamento di dati personali, effettuate da Facebook dopo la loro trasmissione a quest'ultima, in quanto il gestore del sito internet non era in grado di determinare le finalità e i mezzi di tali operazioni in virtù dell'integrazione del plug-in sociale:

"Per contro, alla luce di dette informazioni, risulta escluso, a prima vista, che la Fashion ID determini le finalità e gli strumenti delle successive operazioni di trattamento di dati personali, effettuate dalla Facebook Ireland dopo la loro trasmissione a quest'ultima, cosicché la Fashion ID non può essere considerata responsabile di tali operazioni [...]"[39].

38. In caso di contitolarità del trattamento, ai sensi dell'articolo 26, paragrafo 1, GDPR, i titolari del trattamento sono tenuti a mettere in atto un accordo che, in modo trasparente, determini le rispettive responsabilità ai fini del rispetto del GDPR, in particolare per quanto concerne l'esercizio dei diritti dell'interessato e gli obblighi di fornire le informazioni di cui agli articoli 13 e 14 GDPR.

39. Le sezioni che seguono chiariscono, attraverso esempi specifici, i ruoli dei *targeter* e dei fornitori di social media in relazione ai diversi meccanismi di *targeting*. Considerazioni specifiche sono svolte, in particolare, sull'applicazione dei requisiti di liceità e di limitazione della finalità in questo contesto. Successivamente vengono analizzati i requisiti relativi alla trasparenza, alle valutazioni d'impatto sulla protezione dei dati e al trattamento di categorie particolari di dati. Infine le linee guida esaminano l'obbligo per i contitolari del trattamento di mettere in atto un accordo adeguato ai sensi dell'articolo 26 GDPR, tenendo conto del livello di responsabilità del *targeter* e del fornitore di social media.

5. ANALISI DEI DIVERSI MECCANISMI DI *TARGETING*

5.1 PANORAMICA

40. Gli utenti di social media possono essere soggetti ad attività di *targeting* sulla base di dati forniti, osservati o desunti, così come di una loro combinazione:

    a) ***targeting* di persone fisiche sulla base di dati forniti** – "dati forniti" si riferisce alle informazioni fornite attivamente dall'interessato al fornitore di social media e/o al *targeter*[40]. Ad esempio:

- un utente di social media potrebbe indicare la propria età nella descrizione del suo profilo utente. Il fornitore di social media, a sua volta, potrebbe consentire il *targeting* sulla base di tale criterio;
- un *targeter* potrebbe utilizzare le informazioni fornite dall'interessato al *targeter* al fine di rivolgersi in maniera mirata a tale persona, ad esempio attraverso i dati dei clienti (quali un elenco di indirizzi di posta elettronica), da abbinare ai dati già in possesso della piattaforma di social media, facendo sì che tutti gli utenti che corrispondono a tali dati ricevano pubblicità mirata[41];

b) ***targeting* sulla base di dati osservati** – il *targeting* degli utenti di social media può avvenire anche sulla base di dati osservati[42]. I dati osservati sono dati forniti dall'interessato in virtù dell'utilizzo di un servizio o di un dispositivo[43]. Ad esempio un particolare utente dei social media potrebbe essere oggetto di attività di *targeting* sulla base de:

- la sua attività sulla piattaforma di social media stessa (ad esempio i contenuti che l'utente ha condiviso, consultato o dichiarato di apprezzare tramite "mi piace" o pulsanti analoghi);
- l'uso di dispositivi sui quali viene eseguita l'applicazione del social media (ad esempio coordinate GPS, numero di telefono cellulare);
- dati ottenuti da uno sviluppatore di applicazioni di terze parti utilizzando le interfacce di programmazione delle applicazioni (API) o i kit di sviluppo del software (SDK) offerti da fornitori di social media;
- dati raccolti attraverso siti web di terzi che hanno incorporato plugin sociali o pixel;
- dati raccolti tramite altri terzi (ad esempio soggetti con i quali l'interessato ha interagito, dai quali ha acquistato un prodotto, con i quali ha sottoscritto carte fedeltà); oppure
- dati raccolti attraverso servizi offerti da imprese di proprietà o gestite dal fornitore di social media;

c) ***targeting* sulla base di dati desunti** – i "dati desunti" o "dati derivati" sono creati dal titolare del trattamento sulla base dei dati forniti dall'interessato od osservati dal titolare del trattamento[44]. Ad esempio un fornitore di social media o un *targeter* potrebbe dedurre che una persona fisica è probabilmente interessata a una determinata attività o a un certo prodotto sulla base del suo comportamento di navigazione in internet e/o dei suoi collegamenti di rete.

5.2 *TARGETING* SULLA BASE DI DATI FORNITI

5.2.1 DATI FORNITI DALL'UTENTE AL FORNITORE DI SOCIAL MEDIA

41. Le persone fisiche possono comunicare attivamente una quantità notevole di informazioni su se stesse quando utilizzano i social media. La creazione di un account di social media (o "profilo") comporta la comunicazione di una

serie di attributi, tra i quali possono figurare nome, data di nascita, sesso, luogo di residenza, lingua, ecc. A seconda della natura della piattaforma di social media, gli utenti possono includere ulteriori informazioni quali lo stato di relazione, gli interessi o l'occupazione attuale. I dati personali forniti dagli utenti di social media possono essere utilizzati dal fornitore di social media per sviluppare criteri che consentono al *targeter* di indirizzare messaggi specifici agli utenti di tale social media.

Esempio 1

L'impresa X vende calzature da uomo e desidera promuovere i saldi per la propria collezione invernale. Per la propria campagna pubblicitaria desidera rivolgersi a uomini tra i 30 e i 45 anni che hanno indicato di essere single nel loro profilo sui social media. Utilizza quindi i criteri di *targeting* corrispondenti offerti dal fornitore di social media come parametri per identificare la platea di destinatari al quale la propria pubblicità dovrebbe essere resa visibile. Inoltre il *targeter* indica che la pubblicità dovrebbe essere resa visibile agli utenti di social media mentre stanno utilizzando il servizio di social media tra le ore 17:00 e le 20:00. Per consentire il *targeting* degli utenti di social media sulla base di criteri specifici, il fornitore di social media ha precedentemente determinato quali tipi di dati personali saranno utilizzati per sviluppare i criteri di *targeting* e quali criteri di *targeting* saranno offerti. Il fornitore di social media comunica inoltre alcune informazioni statistiche una volta che la pubblicità è stata visualizzata dalla platea dei destinatari (ad esempio per segnalare la composizione demografica delle persone fisiche che hanno interagito con la pubblicità).

A. Ruoli

42. Nell'esempio 1 tanto il *targeter* quanto il fornitore di social media partecipano alla determinazione della finalità e dei mezzi del trattamento di dati personali. Ciò si traduce nel mostrare la pubblicità al pubblico destinatario.

43. Per quanto riguarda la determinazione della *finalità*, l'impresa X e il fornitore di social media determinano congiuntamente la finalità del trattamento, che consiste nel mostrare una pubblicità specifica a un insieme di persone fisiche (in questo caso gli utenti di social media) che costituiscono la platea dei destinatari, scegliendo i criteri di *targeting* disponibili associati a tali utenti al fine di raggiungere una platea verosimilmente interessata e di fornire contenuti pubblicitari più pertinenti. Inoltre esiste anche un vantaggio reciproco derivante dal trattamento stesso che costituisce un ulteriore indicatore del fatto che le finalità perseguite dall'impresa X e dal fornitore di social media sono indissolubilmente legati[45].

44. Per quanto concerne la determinazione dei *mezzi*, il *targeter* e il fornitore di social media determinano congiuntamente i mezzi, un'attività che sfocia nel *targeting*. Il *targeter* partecipa alla determinazione dei mezzi scegliendo di utilizzare i servizi offerti dal fornitore di social media e chiedendogli di

rivolgersi in maniera mirata a un pubblico in base a determinati criteri (ad esempio fascia di età, stato di relazione, orari di visualizzazione)[47]. In questo modo il *targeter* definisce i criteri in base ai quali si svolge il *targeting* e designa le categorie di persone i cui dati personali saranno utilizzati. Il fornitore di social media, d'altra parte, ha deciso di trattare i dati personali dei suoi utenti in modo tale da sviluppare i criteri di *targeting* che mette a disposizione del *targeter*[48]. Per procedere in tal senso il fornitore di social media ha preso alcune decisioni riguardanti i mezzi essenziali del trattamento, come ad esempio quali categorie di dati saranno trattati, quali criteri di *targeting* saranno offerti e chi avrà accesso a (quali tipi di) dati personali che sono trattati nel contesto di una particolare campagna di *targeting*[49].

45. Per ragioni di completezza, l'EDPB sottolinea che il fornitore di social media non si configura come responsabile del trattamento ai sensi dell'articolo 4, paragrafo 8, GDPR[50]. Nell'esempio 1, i criteri di *targeting* sviluppati dal fornitore di social media sulla base dei dati personali dell'utente possono essere utilizzati dal fornitore di social media per operazioni di trattamento future, circostanza questa che dimostra che quest'ultimo non può qualificarsi come responsabile del trattamento. Inoltre il fornitore di social media non sembra trattare i dati esclusivamente per conto dell'impresa X e secondo le istruzioni di quest'ultima.

46. La contitolarità tra il *targeter* e il fornitore di social media si estende soltanto a quei trattamenti per i quali essi determinano concretamente e congiuntamente le finalità e i mezzi. Si estende al trattamento dei dati personali risultanti dalla selezione dei criteri di *targeting* pertinenti e alla presentazione della pubblicità al pubblico destinatario. Copre inoltre il trattamento dei dati personali intrapreso dal fornitore di social media per riferire al *targeter* i risultati della campagna di *targeting*. La contitolarità non si estende, tuttavia, alle operazioni che comportano il trattamento di dati personali in altre fasi precedenti la selezione dei criteri di *targeting* pertinenti o successive al completamento delle attività di *targeting* e della relativa rendicontazione (quali lo sviluppo di nuovi criteri di *targeting* da parte del fornitore di social media sulla base di campagne di *targeting* completate) nonché nelle fasi in cui il *targeter* non ha partecipato alla determinazione delle finalità e dei mezzi, così come il fornitore di social media, in linea di principio, non partecipa alla fase di pianificazione di una campagna di *targeting* prima del momento in cui il *targeter* prende contatto con il fornitore di social media[51].

47. L'analisi di cui sopra resta valida anche se il *targeter* specifica soltanto i parametri della sua platea di destinatari e non ha accesso ai dati personali degli utenti che sono interessati. In effetti la responsabilità congiunta di più soggetti in relazione a un medesimo trattamento non richiede che ciascuno di essi abbia accesso ai dati personali in questione[52]. L'EDPB ricorda che l'accesso concreto ai dati personali non è un prerequisito per la responsabilità congiunta[53].

B. Base giuridica

48. In qualità di contitolari del trattamento, entrambe le parti (il fornitore di social media e il *targeter*) devono essere in grado di dimostrare l'esistenza di

una base giuridica (articolo 6 GDPR) per giustificare il trattamento dei dati personali di cui ciascuno dei contitolari è responsabile. L'EDPB ricorda che non viene definita alcuna gerarchia specifica tra le diverse basi giuridiche del GDPR: il titolare del trattamento deve assicurarsi che la base giuridica selezionata corrisponda all'obiettivo e al contesto del trattamento in questione. L'individuazione della base giuridica appropriata è legata ai principi di correttezza e limitazione delle finalità[54].

49. In generale vi sono due basi giuridiche che potrebbero giustificare il trattamento a sostegno del *targeting* degli utenti di social media: il consenso dell'interessato (articolo 6, paragrafo 1, lettera a), GDPR) oppure interessi legittimi (articolo 6, paragrafo 1, lettera f), GDPR). Un titolare del trattamento deve sempre considerare quale sia la base giuridica appropriata nelle circostanze specifiche. Per quanto concerne i fornitori di social media, l'articolo 6, paragrafo 1, lettera b), GDPR non può fornire una base giuridica per la pubblicità online semplicemente perché tale pubblicità finanzia indirettamente la fornitura del loro servizio[55]. Lo stesso vale per il *targeter* in quanto il *targeting* degli utenti di social media non può essere considerato un elemento intrinseco e atteso di taluni servizi o necessario per eseguire un contratto con l'utente[56]. Mentre la personalizzazione del contenuto, in alcune circostanze, può costituire un elemento intrinseco e atteso di alcuni servizi online[57], l'articolo 6, paragrafo 1, lettera b), GDPR nel contesto del *targeting* degli utenti di social media è difficilmente applicabile, come illustrato negli esempi di cui alle presenti linee guida[58].

50. Per quanto riguarda la base giuridica del legittimo interesse, l'EDPB ricorda che nella sentenza *Fashion ID*, la Corte ha ribadito che, affinché un trattamento possa basarsi sul legittimo interesse, devono essere soddisfatte tre condizioni cumulative, ossia:[59] i) il perseguimento del legittimo interesse del titolare del trattamento oppure del o dei terzi cui vengono comunicati i dati; ii) la necessità del trattamento dei dati personali per il perseguimento del legittimo interesse; e iii) la condizione che non prevalgano i diritti e le libertà fondamentali della persona interessata dalla tutela dei dati. La Corte ha inoltre precisato che in una situazione di contitolarità "*è necessario che ciascuno di tali titolari persegua, con le operazioni di trattamento succitate, un interesse legittimo [...] al fine di poter addurre una giustificazione per dette operazioni*"[60].

51. Per quanto riguarda l'esempio 1, il *targeter* potrebbe considerare un suo legittimo interesse quello di ottenere maggiore pubblicità per i suoi prodotti attraverso il *targeting* sui social media. Il fornitore di social media potrebbe considerare che un suo legittimo interesse quello di rendere redditizio il servizio di social media attraverso la vendita di spazi pubblicitari. La possibilità per il *targeter* e il fornitore di social media di invocare l'articolo 6, paragrafo 1, lettera f), GDPR come base giuridica dipende dal fatto che tutte e tre le condizioni cumulative siano soddisfatte, come recentemente ribadito dalla Corte. Anche se il *targeter* e il fornitore di social media considerano legittimi i rispettivi interessi economici, ciò non significa necessariamente che potranno effettivamente fare affidamento sull'articolo 6, paragrafo 1, lettera f), GDPR.

52. La seconda parte del test comparativo implica che i contitolari del trattamento dovranno stabilire che il trattamento è necessario per conseguire tali legittimi interessi. Tale "necessarietà" richiede l'esistenza di un legame tra il trattamento e i legittimi interessi perseguiti. Il requisito della "necessarietà" è particolarmente rilevante nel contesto dell'applicazione dell'articolo 6, paragrafo 1, lettera f), al fine di garantire che il trattamento dei dati basato su legittimi interessi non comporti un'interpretazione indebitamente ampia della necessità di trattare i dati. Come negli altri casi, ciò significa che occorre valutare se esistono altri mezzi meno invasivi per conseguire lo stesso obiettivo.

53. La terza fase della valutazione dell'eventualità che il *targeter* e il fornitore di social media possano invocare l'articolo 6, paragrafo 1, lettera f), GDPR come base giuridica per il trattamento dei dati personali, è costituita dal test comparativo necessario per determinare se il legittimo interesse in gioco prevalga sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato[62].

54. L'EDPB ricorda che ove un titolare del trattamento preveda di invocare un legittimo interesse, i doveri di trasparenza e il diritto di opposizione richiedono un'attenta considerazione. Gli interessati dovrebbero avere la possibilità di opporsi al trattamento dei loro dati per finalità specifiche prima che il trattamento venga avviato. Gli utenti di social media dovrebbero non soltanto avere la possibilità di opporsi alla visualizzazione di pubblicità mirata quando accedono alla piattaforma, ma anche disporre di controlli che garantiscano che il trattamento sottostante dei loro dati personali per la finalità di *targeting* non abbia più luogo in seguito alla loro opposizione.

55. Il *targeter* che intenda fare affidamento sul legittimo interesse dovrebbe, da parte sua, facilitare l'espressione di una previa opposizione degli utenti di social media rispetto all'utilizzo che tale *targeter* intende compierne per finalità di *targeting* . Tuttavia, nella misura in cui non interagisce direttamente con l'interessato, il *targeter* dovrebbe quanto meno assicurarsi che la piattaforma di social media fornisca all'interessato gli strumenti per esercitare efficacemente il suo diritto di opposizione preventiva. In qualità di contitolari del trattamento, il *targeter* e il fornitore di social media dovrebbero chiarire in che modo il diritto di opposizione delle persone fisiche (così come altri diritti) saranno gestiti nel contesto dell'accordo di contitolarità (cfr. sezione 6). Se dal test comparativo emerge che gli interessi oppure i diritti e le libertà fondamentali degli interessati prevalgono sul legittimo interesse del fornitore di social media e del *targeter*, non è possibile invocare l'articolo 6, paragrafo 1, lettera f).

56. Per quanto riguarda la base giuridica del consenso, il titolare del trattamento deve tenere a mente che ci sono chiaramente situazioni nelle quali il trattamento non sarebbe lecito senza il consenso valido degli interessati (articolo 6, paragrafo 1, lettera a), GDPR). Ad esempio il Gruppo di lavoro ha precedentemente ritenuto che sarebbe difficile per i titolari del trattamento giustificare il ricorso al legittimo interesse quale base giuridica per pratiche intrusive di profilazione e tracciamento per finalità di marketing o pubblicità, come quelle che comportano il tracciamento di persone fisiche su più siti web, ubicazioni, dispositivi, servizi o l'intermediazione di dati[63].

57. Per essere valido il consenso raccolto per il trattamento deve soddisfare le condizioni di cui all'articolo 4, paragrafo 11, e all'articolo 7 GDPR. In generale il consenso può costituire una base giuridica adeguata soltanto se all'interessato vengono assicurati il controllo e una scelta effettiva. Qualora il consenso costituisca parte integrante e non negoziabile di termini e condizioni, si presume che non sia stato conferito liberamente. Il consenso deve inoltre essere specifico, informato e inequivocabile e l'interessato deve poterlo rifiutare o revocare senza subire pregiudizio[64].

58. Il consenso (articolo 6, paragrafo 1, lettera a), GDPR) potrebbe essere utilizzabile, a condizione che siano soddisfatte tutte le prescrizioni per la sua validità. L'EDPB ricorda che l'ottenimento del consenso non fa inoltre venir meno né diminuisce in alcun modo l'obbligo del titolare del trattamento di rispettare i principi applicabili al trattamento sanciti nel GDPR, in particolare all'articolo 5, per quanto concerne la correttezza, la necessità e la proporzionalità, nonché la qualità dei dati. Anche quando il trattamento dei dati personali si basa sul consenso dell'interessato, ciò non legittimerebbe un *targeting* sproporzionato o iniquo[65].

59. Infine l'EDPB ritiene che il trattamento dei dati personali descritto nell'esempio 1 non possa trovare fondamento nell'articolo 6, paragrafo 1, lettera b), né per quanto riguarda la piattaforma sociale né per quanto riguarda il *targeter*[66].

5.2.2 DATI FORNITI AL TARGETER DALL'UTENTE DELLA PIATTAFORMA DI SOCIAL MEDIA

60. Il *targeting* può altresì comportare dati forniti dall'interessato al *targeter*, che poi utilizza i dati raccolti per rivolgersi in maniera mirata all'interessato sui social media. Ad esempio il *targeting* "basato su elenchi" si verifica quando un *targeter* carica elenchi preesistenti di dati personali (quali indirizzi di posta elettronica o numeri di telefono) affinché il fornitore di social media li abbini alle informazioni disponibili sulla piattaforma. In questo caso il fornitore di social media confronta i dati caricati dal *targeter* con i dati degli utenti che già possiede, e gli utenti che corrispondono vengono aggiunti o esclusi dal pubblico destinatario (ossia dal "gruppo" di persone al quale verrà mostrata la pubblicità sulla piattaforma di social media). Il fornitore di social media può inoltre consentire al *targeter* di "verificare" l'elenco prima di finalizzarlo, il che significa che avviene un determinato trattamento anche prima della definizione della platea di destinatari.

Esempio 2

La signora Jones contatta la banca X per fissare un appuntamento per un possibile mutuo perché sta acquistando una casa. Contatta la banca via posta elettronica per fissare l'appuntamento. Dopo l'appuntamento, la signora Jones decide di non diventare cliente della banca. La banca ha comunque aggiunto l'indirizzo di posta elettronica della signora Jones al database

di indirizzi di posta elettronica, consentendo al fornitore di social media di "abbinare" l'elenco di indirizzi di posta elettronica in suo possesso con gli indirizzi detenuti dalla piattaforma di social media, al fine di rivolgersi in maniera mirata alle persone in questione con l'intera gamma di servizi finanziari sulla piattaforma di social media.

Esempio 3

Il signor Lopez è cliente della banca X da quasi un anno. Quando è diventato cliente, ha fornito un indirizzo di posta elettronica ed è stato informato dalla banca X, al momento della raccolta di tale dato, che: a) il suo indirizzo di posta elettronica sarebbe stato utilizzato per l'invio di pubblicità in merito a offerte legate ai servizi bancari che sta già utilizzando; e b) potrà opporsi a tale trattamento in qualsiasi momento. La banca ha aggiunto il suo indirizzo di posta elettronica al database degli indirizzi di posta elettronica dei clienti. In seguito la banca utilizza tale database di indirizzi di posta elettronica per rivolgersi in maniera mirata ai suoi clienti sulla piattaforma di social media con l'intera gamma di servizi finanziari che essa offre[67].

A. Ruoli

61. In questi esempi, il *targeter*, ossia la banca, agisce in veste di titolare del trattamento dato che determina le finalità e i mezzi del trattamento raccogliendo, elaborando e trasmettendo attivamente i dati personali degli interessati al fornitore di social media per finalità pubblicitarie. Il fornitore di social media, a sua volta, agisce in veste di titolare del trattamento avendo preso la decisione di utilizzare i dati personali acquisiti dall'utente del social media (ossia l'indirizzo di posta elettronica fornito al momento della creazione del suo account) al fine di consentirgli di mostrare pubblicità a un pubblico di persone fisiche specifiche.

62. La contitolarità esiste in relazione ai trattamenti per i quali il fornitore di social media e il *targeter* determinano congiuntamente le finalità e i mezzi. Nel caso di specie, ciò comprende il caricamento di identificatori unici relativi al pubblico destinatario, l'abbinamento, la selezione dei criteri di *targeting* e la successiva visualizzazione della pubblicità, nonché l'eventuale rendicontazione relativa alla campagna di *targeting*[68].

63. In entrambi gli esempi la banca agisce come unico titolare del trattamento per quanto riguarda la raccolta iniziale degli indirizzi di posta elettronica rispettivamente della signora Jones e del signor Lopez. Il fornitore di social media non partecipa in alcun modo a determinare i mezzi e le finalità di tale raccolta. La contitolarità inizia con la trasmissione dei dati personali e la loro simultanea raccolta da parte del fornitore di social media. Continua per tutta la durata della visualizzazione della pubblicità mirata e termina (nella maggior parte dei casi) quando viene completata una successiva fase di ren-

dicontazione. In alcuni casi la contitolarità può essere ulteriormente estesa, anche fino alla fase di cancellazione dei dati, nella misura in cui il *targeter* continui a partecipare alla determinazione delle finalità e dei mezzi.

64. Il motivo per cui la banca agisce come unico titolare del trattamento quando raccoglie gli indirizzi di posta elettronica rispettivamente della signora Jones e del signor Lopez, dipende dal fatto che la raccolta dei dati avviene prima della campagna di *targeting* (e non è indissolubilmente legata a quest'ultima). Di conseguenza, nel caso di specie si deve distinguere tra un trattamento iniziale, per il quale soltanto la banca è titolare, e un trattamento successivo per il quale sussiste una contitolarità. La responsabilità della banca non si estende alle operazioni che avvengono dopo che il *targeting* e la rendicontazione sono stati completati e per le quali il *targeter* non ha partecipato alla definizione delle finalità e dei mezzi; rispetto a tali operazioni, il fornitore di social media agisce come unico titolare del trattamento.

B. Base giuridica

65. Nell'esempio 2, l'articolo 6, paragrafo 1, lettera f), GDPR non costituisce una base giuridica adeguata per giustificare il trattamento nel caso specifico, tenendo conto del contesto in cui i dati personali sono stati forniti. In effetti la signora Jones ha contattato la banca alla sola finalità di fissare un appuntamento, dopo di che ha comunicato la sua intenzione di non usufruire dei servizi offerti dalla banca. Di conseguenza si può ritenere che la signora Jones non si aspetti affatto che i suoi dati personali vengano utilizzati per finalità di *targeting* ("*ritargeting*"). Inoltre un test di compatibilità ai sensi dell'articolo 6, paragrafo 4, GDPR indicherebbe probabilmente che tale trattamento non è compatibile con la finalità per la quale sono stati inizialmente raccolti i dati personali.

66. Nell'esempio 3 il *targeter* potrebbe invocare un legittimo interesse per giustificare il trattamento, tenendo conto tra l'altro degli elementi seguenti: a) il signor Lopez era informato del fatto che il suo indirizzo di posta elettronica avrebbe potuto essere utilizzato per finalità pubblicitarie tramite i social media per servizi collegati a quello utilizzato dall'interessato; b) la pubblicità avrebbe riguardato servizi analoghi a quelli di cui il signor Lopez è già cliente; e c) il signor Lopez ha avuto la possibilità di opporsi prima del trattamento, al momento della raccolta dei suoi dati personali da parte dalla banca. Tuttavia l'EDPB intende evidenziare che l'adempimento dei doveri di informazione a norma degli articoli 13 e 14 GDPR e la ponderazione degli interessi da effettuare ai sensi dell'articolo 6 paragrafo 1, lettera f), GDPR rappresentano due distinti obblighi. Di conseguenza il mero adempimento dei doveri di informazione a norma degli articoli 13 e 14 del GDPR non costituisce una misura di trasparenza da prendere in considerazione per la ponderazione degli interessi conformemente all'articolo 6, paragrafo 1, lettera f), GDPR.

5.3 *TARGETING* SULLA BASE DI DATI OSSERVATI

67. Esistono molti modi in cui i fornitori di social media possono osservare il comportamento dei loro utenti. Ad esempio l'osservazione è possibile attraverso il servizio di social media stesso o può anche essere possibile su siti web esterni in virtù di plug-in sociali o pixel.

Esempio 4 *Targeting* basato su pixel

Il signor Schmidt sta navigando online per acquistare uno zaino. Visita il sito web "MiglioriBorse.com", vede un certo numero di articoli, ma decide di non effettuare un acquisto. Il gestore di "MiglioriBorse.com" desidera rivolgersi in maniera mirata agli utenti di social media che hanno visitato il loro sito web senza effettuare un acquisto. A tal fine integra un cosiddetto "pixel di tracciamento"[69] sul proprio sito web, che viene messo a disposizione dal fornitore di social media. Dopo aver lasciato il sito web di MiglioriBorse.com e aver effettuato l'accesso al suo account di social media, il signor Schmidt comincia a vedere la pubblicità degli zaini che stava considerando quando navigava su MiglioriBorse.com.

Esempio 5 *Geotargeting*

La signora Michu ha installato l'applicazione di un fornitore di social media sul suo smartphone. Cammina per Parigi durante le sue vacanze. Il fornitore di social media raccoglie informazioni sulla posizione della signora Michu attraverso le funzionalità GPS del suo smartphone su base continuativa[70] utilizzando i permessi che sono stati concessi al fornitore di social media quando l'applicazione è stata installata. La signora Michu alloggia in un hotel che si trova accanto a una pizzeria. La pizzeria utilizza la funzionalità di *geotargeting* offerta dal fornitore di social media per rivolgersi in maniera mirata alle persone fisiche che si trovano entro 1 km dai suoi locali per la prima volta negli ultimi 6 mesi. Aprendo l'applicazione del fornitore di social media sul proprio smartphone, la signora Michu vede una pubblicità della pizzeria, decide che ha fame e compra una pizza tramite il suo sito web.

Esempio 6

La signora Ghorbani crea un account su una piattaforma di social media. Durante il processo di registrazione le viene chiesto se acconsente al trattamento dei suoi dati personali per vedere pubblicità mirata sulla sua pagina di social media, sulla base dei dati che fornisce direttamente al fornitore di social media (come l'età, il sesso e l'ubicazione), così come sulla base della sua attività su altri siti web al di fuori della piattaforma di social media attraverso cookie. Viene informata che tali dati saranno raccolti tramite pixel

di tracciamento o plug-in sociali di social media, i processi le sono descritti chiaramente, così come il fatto che il *targeting* coinvolge altre entità che sono congiuntamente responsabili di garantire il rispetto del GDPR. Le viene anche spiegato che può revocare il proprio consenso in qualsiasi momento e le viene fornito un collegamento ipertestuale per visionare la politica sulla tutela della vita privata. Dato che la signora Ghorbani è interessata a vedere pubblicità mirata sulla propria pagina di social media, fornisce il proprio consenso. Non viene installato o raccolto alcun cookie pubblicitario finché la signora Ghorbani non esprime il proprio consenso.

Più tardi visita il sito web "Leultimenotizie.com" che presenta un pulsante del social media integrato su di esso. Un banner di piccole dimensioni ma ben visibile appare sul bordo destro dello schermo chiedendo alla signora Ghorbani di acconsentire alla trasmissione dei suoi dati personali al fornitore di social media tramite cookie e il plug-in del social media. Il gestore del sito web ha adottato misure tecniche affinché nessun dato personale sia trasferito alla piattaforma di social media fino a quando lei non fornisce il suo consenso.

5.3.1 RUOLI

68. Nell'esempio 4 tanto il *targeter* quanto il fornitore di social media partecipano alla determinazione delle finalità e dei mezzi del trattamento dei dati personali, il che si traduce nella visualizzazione della pubblicità da parte del signor Schmidt.

69. Per quanto riguarda la determinazione delle finalità, MiglioriBorse.com e il fornitore di social media determinano congiuntamente la finalità del trattamento, che consiste nel rendere visibile una pubblicità specifica sulla piattaforma di social media alle persone che costituiscono il pubblico destinatario. Integrando il pixel nel proprio sito web, MiglioriBorse.com esercita un'influenza decisiva sui mezzi del trattamento. La raccolta e la trasmissione dei dati personali dei visitatori del sito web al fornitore di social media non sarebbero avvenute senza l'integrazione di tale pixel. Il fornitore di social media, d'altra parte, ha sviluppato e offre il codice software (pixel) che porta alla raccolta, alla trasmissione e alla valutazione automatiche per finalità di marketing dei dati personali al fornitore di social media. Di conseguenza esiste una contitolarità in relazione alla raccolta dei dati personali e alla loro trasmissione tramite pixel, così come in relazione all'abbinamento e alla successiva presentazione della pubblicità al signor Schmidt sulla piattaforma sociale così come per qualsiasi attività di rendicontazione relativa alla campagna di *targeting*. La contitolarità esiste anche nell'esempio 6, per ragioni analoghe.

70. Nell'esempio 5 la pizzeria esercita un'influenza decisiva sul trattamento dei dati personali definendo i parametri del *targeting* pubblicitario secondo le proprie esigenze commerciali (ad esempio gli orari di apertura della pizzeria

e la geolocalizzazione delle persone vicine alla pizzeria in tale fascia oraria) e deve quindi essere considerata partecipe della determinazione delle finalità e dei mezzi del trattamento. Il fornitore di social media, d'altra parte, ha raccolto le informazioni relative alla posizione della signora Michu (tramite GPS) per la propria finalità di consentire tale pubblicità mirata basata sull'ubicazione. Di conseguenza esiste una contitolarità tra il *targeter* e la piattaforma sociale in relazione alla raccolta e all'analisi dell'ubicazione della signora Michu, nonché alla visualizzazione della pubblicità, al fine di rivolgersi in maniera mirata a lei (come persona che appare entro 1 km dalla pizzeria per la prima volta negli ultimi 6 mesi) tramite la pubblicità.

5.3.2 BASE GIURIDICA

71. Innanzitutto, dato che gli esempi 4, 5 e 6 implicano l'uso di cookie, occorre prendere in considerazione i requisiti derivanti dall'articolo 5, paragrafo 3, della direttiva e-privacy.

72. A tale proposito occorre osservare che l'articolo 5, paragrafo 3, della direttiva e-privacy richiede che gli utenti siano informati in modo chiaro e completo tra l'altro sulle finalità del trattamento, prima di esprimere il proprio consenso[71], salvo eccezioni molto limitate[72]. Informazioni chiare e complete implicano che un utente sia in grado di determinare facilmente le conseguenze di qualsiasi consenso che possa fornire ed assicurarsi che il consenso dato sia ben informato[73]. Di conseguenza il titolare del trattamento dovrà informare gli interessati in merito a tutte le finalità pertinenti, compreso qualsiasi trattamento successivo dei dati personali ottenuti accedendo alle informazioni nell'apparecchiatura terminale.

73. Ai fini della sua validità, il consenso raccolto per l'implementazione di tecnologie di tracciamento deve soddisfare le condizioni di cui all'articolo 7 GDPR[74]. Ad esempio il consenso non è validamente prestato se l'uso dei cookie è consentito da una casella di spunta preselezionata dal fornitore di servizi, che l'utente deve deselezionare per rifiutare il proprio consenso[75]. In base al considerando 32, azioni quali scorrere un sito o sfogliarne le pagine o azioni analoghe dell'utente non potranno in alcun caso soddisfare il requisito di un'azione positiva inequivocabile: azioni di questo tipo possono essere difficili da distinguere da altre azioni o interazioni dell'utente e quindi non permettono di stabilire che è stato ottenuto un consenso inequivocabile. Inoltre, in un caso del genere, sarà difficile dare all'utente la possibilità di revocare il consenso con la stessa facilità con cui lo ha espresso[76].

74. Qualsiasi (con)titolare del trattamento che intenda fare affidamento sul consenso come base giuridica è tenuto ad accertarsi che sia stato ottenuto un consenso valido. Nella sentenza *Fashion ID* la Corte ha sottolineato l'importanza di garantire la tutela efficace e tempestiva dei diritti dell'interessato nonché di evitare che il consenso sia prestato unicamente al contitolare del trattamento che interviene successivamente. Il consenso valido deve essere ottenuto prima del trattamento, il che implica che i (con)titolari del tratta-

mento devono valutare quando e come fornire le informazioni e ottenere il consenso. In altre parole la questione in merito a quale dei contitolari debba essere incaricato di raccogliere il consenso equivale in ultima analisi a stabilire chi di loro interagisca per primo con l'interessato. Nell'esempio 6, dato che l'installazione di cookie e il trattamento dei dati personali avvengono al momento della creazione dell'account, il fornitore di social media deve raccogliere il consenso valido dell'interessata prima dell'installazione di cookie pubblicitari.

75. L'EDPB ricorda inoltre che qualora più titolari del trattamento (congiunti) intendano basarsi sul medesimo consenso oppure qualora i dati debbano essere trasferiti o trattati da altri titolari del trattamento che intendono basarsi sul consenso iniziale, tutti questi titolari del trattamento devono essere indicati[77]. Nella misura in cui non tutti i contitolari del trattamento siano noti nel momento in cui il fornitore di social media chiede il consenso, quest'ultimo dovrà necessariamente essere integrato da ulteriori informazioni e dal consenso raccolto dal gestore del sito web sul quale viene integrato il plugin per i social media (ossia *Leultimenotizie.com* nell'esempio 6).

76. L'EDPB sottolinea che il consenso che dovrebbe essere raccolto dal gestore del sito web per la trasmissione di dati personali attivata dal suo sito web (integrando un plug-in sociale) si riferisce soltanto all'operazione o all'insieme di operazioni che comportano il trattamento di dati personali per le quali il gestore determina effettivamente le finalità e i mezzi[78]. La raccolta del consenso da parte del gestore di un sito web, ad esempio "Leultimenotizie.com" di cui all'esempio 6, non annulla né riduce in alcun modo l'obbligo del fornitore di social media di assicurarsi che l'interessato abbia fornito un consenso valido per il trattamento di cui è responsabile in qualità di contitolare[79], nonché per qualsiasi trattamento successivo o ulteriore effettuato da tale fornitore e per il quale il gestore del sito web non determina congiuntamente le finalità e i mezzi (ad esempio operazioni successive di profilazione per finalità di *targeting*).

77. Inoltre qualsiasi trattamento successivo di dati personali, compresi i dati personali ottenuti da cookie, plug-in sociali o pixel, deve avere altresì una base giuridica ai sensi dell'articolo 6 GDPR per essere considerato lecito[80]. Per quanto riguarda la base giuridica del trattamento negli esempi 4, 5 e 6, l'EDPB ritiene che il legittimo 'interesse non possa costituire un'idonea base giuridica, dato che il *targeting* si basa sul monitoraggio del comportamento delle persone fisiche attraverso siti web e ubicazioni utilizzando tecnologie di tracciamento[81].

78. Di conseguenza, in tali circostanze, è probabile che la base giuridica appropriata anche per qualsiasi trattamento successivo ai sensi dell'articolo 6 GDPR sia il consenso dell'interessato. In effetti, nel valutare la conformità rispetto all'articolo 6 GDPR, si dovrebbe tener conto del fatto che il trattamento nel suo complesso comporta attività specifiche per le quali il legislatore dell'UE ha cercato di fornire una protezione aggiuntiva[82]. Inoltre i titolari del trattamento devono prendere in considerazione l'impatto sui diritti degli interessati nel definire un'idonea base giuridica, in maniera da rispettare il principio di correttezza[83].

5.4 *TARGETING* SULLA BASE DI DATI DESUNTI

79. I dati desunti si riferiscono ai dati che sono creati dal titolare del trattamento sulla base dei dati forniti dall'interessato (indipendentemente dal fatto che tali dati siano stati osservati o forniti attivamente dall'interessato o siano una loro combinazione)[84]. Inferenze in merito agli interessati possono essere compiute tanto dal fornitore di social media quanto dal *targeter*.

80. Ad esempio monitorando il comportamento dei suoi utenti per un lungo periodo di tempo, tanto sul social media quanto al di fuori di tale contesto (ad esempio pagine visitate, tempo trascorso su ogni pagina, numero di riconnessioni a tale pagina, parole cercate, collegamenti ipertestuali seguiti, "Mi piace" indicati), il fornitore di social media può essere in grado di dedurre informazioni riguardanti gli interessi e altre caratteristiche dell'utente del social media. Analogamente un *targeter* potrebbe essere in grado di dedurre informazioni su persone specifiche e utilizzare tale conoscenza quando si rivolge in maniera mirata a tali persone mostrando pubblicità sulle loro pagine di social media.

Esempio 7

La signora Delucca mette spesso "mi piace" alle foto postate dalla galleria d'arte "Artestupenda" del pittore impressionista Pataolito sulla sua pagina di social media. Il museo Z sta cercando di attirare persone interessate ai dipinti impressionisti in vista della sua prossima mostra. Il museo Z utilizza i seguenti criteri di *targeting* offerti dal fornitore di social media: "interessato all'impressionismo", sesso, età e luogo di residenza. La signora Delucca riceve successivamente una pubblicità mirata da parte del museo Z relativa all'imminente mostra organizzata da tale museo sulla propria pagina di social media.

Esempio 8

Il signor Leon ha indicato nella propria pagina di social media di essere interessato allo sport. Ha scaricato un'applicazione sul proprio cellulare per seguire gli ultimi risultati degli incontri sportivi preferiti, ha impostato sul proprio browser la pagina www.risultatisportiviintemporeale.com come homepage sul suo portatile, usa spesso il desktop di cui dispone sul luogo di lavoro per cercare gli ultimi risultati sportivi su internet. Visita inoltre anche un certo numero di siti web di gioco d'azzardo online. Il fornitore di social media traccia l'attività online del signor Leon sui suoi molteplici dispositivi, ossia sul computer portatile, sul cellulare e sul desktop. Sulla base di tale attività e di tutte le informazioni fornite dal signor Leon, il fornitore di social media deduce che sarà interessato alle scommesse online. Inoltre la piattaforma di social media ha sviluppato criteri di *targeting* che consentono alle imprese di rivolgersi in maniera mirata a persone che probabilmente sono impulsive e hanno un reddito più basso.

La società di scommesse online "miglioriprestitiquotidiani" desidera rivolgersi agli utenti che sono interessati alle scommesse e che probabilmente scommettono somme considerevoli. Seleziona quindi i criteri offerti dal fornitore di social media per rivolgersi in maniera mirata al pubblico al quale dovrebbe essere mostrata la sua pubblicità.

5.4.1 RUOLI

81. Per quanto riguarda la determinazione dei ruoli dei diversi attori, l'EDPB nota quanto segue: nell'esempio 7 esiste una contitolarità tra il museo Z e il fornitore di social media per quanto riguarda il trattamento dei dati personali per finalità di pubblicità mirata, tenendo conto della raccolta di questi dati tramite la funzionalità "mi piace" presente sulla piattaforma di social media nonché l'"analisi" effettuata dal fornitore di social media per offrire il criterio di *targeting* ("interessato all'impressionismo") al destinatario con la finalità di far visualizzare in definitiva la pubblicità[85].

82. Nell'esempio 8 esiste una contitolarità tra "miglioriprestitiquotidiani" e il fornitore di social media in relazione ai trattamenti determinati congiuntamente, in questo caso la selezione dei criteri di *targeting* e la successiva visualizzazione della pubblicità, così come l'eventuale attività di rendicontazione in merito alla campagna di *targeting*.

5.4.2 BASE GIURIDICA

83. Il *targeting* degli utenti di social media per finalità pubblicitarie sulla base di dati desunti comporta in genere la profilazione[86]. Il Gruppo di lavoro ha già chiarito che secondo il GDPR, la profilazione è un trattamento automatizzato di dati personali che mira a valutare aspetti personali, in particolare per analizzare o effettuare previsioni sulle persone fisiche, aggiungendo che "*[l]'uso del verbo 'valutare' suggerisce che la profilazione implichi una qualche forma di valutazione o giudizio in merito a una persona*"[87]. La profilazione può essere legittima in riferimento a uno qualsiasi dei fondamenti giuridici di cui all'articolo 6, paragrafo 1, GDPR, fatta salva la validità di tale base giuridica.

84. Nell'esempio 7, è applicabile l'articolo 5, paragrafo 3, della direttiva e-privacy nella misura in cui la visualizzazione della pubblicità sulla pagina della signora Delucca relativa al pittore Pataolito richiede un'operazione di lettura/scrittura per abbinare il "mi piace" alle informazioni precedentemente detenute su di lei dal fornitore di social media. Per tali operazioni sarà quindi necessario il consenso.

85. Per quanto riguarda l'esempio 8, l'EDPB ricorda che nel caso di un processo decisionale automatizzato che produce effetti giuridici che riguardano l'interessato o che incida in modo analogo significativamente sulla sua persona, come stabilito dall'articolo 22 del GDPR, i titolari del trattamento possono avvalersi delle seguenti eccezioni:

- consenso esplicito dell'interessato;
- necessità del processo decisionale automatizzato ai fini della stipula o dell'esecuzione di un contratto; oppure
- autorizzazione conferita dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

86. Il Gruppo di lavoro ha già dichiarato che *"[i]n numerosi casi tipici, la decisione di proporre pubblicità mirata basata sulla profilazione non inciderà in modo analogo significativamente sulle persone [...]. Tuttavia è possibile che ciò possa accadere, a seconda delle particolari caratteristiche del caso, tra le quali:*

- *l'invasività del processo di profilazione, compreso il tracciamento delle persone su siti web, dispositivi e servizi diversi;*
- *le aspettative e le volontà delle persone interessate;*
- *il modo in cui viene reso disponibile l'annuncio pubblicitario; oppure*
- *lo sfruttamento della conoscenza di vulnerabilità degli interessati coinvolti"*[88].

87. Se la profilazione effettuata dal fornitore di social media può "[incidere] in modo analogo significativamente" su un interessato, si applica l'articolo 22. Il titolare del trattamento (o i contitolari del trattamento, a seconda del caso) dovrà (dovranno) effettuare una valutazione dell'eventualità che il *targeting* "[incida] in modo analogo significativamente" su un interessato, in ogni caso tenendo conto delle caratteristiche concrete del *targeting*.

88. In tali circostanze, come descritto nell'esempio 8, la presentazione di pubblicità di scommesse online può rientrare nell'ambito di applicazione dell'articolo 22 GDPR (attività di *targeting* rivolta a persone finanziariamente vulnerabili interessate a scommesse online, che ha il potenziale di incidere significativamente e negativamente sulla loro situazione finanziaria). Di conseguenza, conformemente all'articolo 22, sarebbe necessario un consenso esplicito. Inoltre l'utilizzo di tecniche di tracciamento fa scattare l'applicabilità dell'articolo 5, paragrafo 3, della direttiva e-privacy, rendendo necessario il preventivo consenso da parte dell'interessato. Infine l'EDPB ricorda che il titolare del trattamento deve condurre una valutazione caso per caso rispetto alla liceità del trattamento, e che l'ottenimento del consenso non riduce gli altri obblighi relativi al rispetto delle prescrizioni in materia di correttezza, necessità, proporzionalità e qualità dei dati, di cui all'articolo 5 GDPR.

6. TRASPARENZA E DIRITTO DI ACCESSO

89. L'articolo 5, paragrafo 1, lettera a), GDPR afferma che i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. L'articolo 5, paragrafo 1, lettera b), GDPR afferma che i dati personali devono essere raccolti per finalità determinate, esplicite e legittime. Gli articoli 12, 13 e 14 del GDPR contengono disposizioni specifiche concernenti gli obblighi di trasparenza del titolare del trattamento dei dati. Infine il considerando 39 recita: *"[d]ovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li*

riguardano nonché la misura in cui i dati personali sono o saranno trattati"[89].

90. Le informazioni presentate agli interessati riguardo alle modalità di trattamento dei loro dati personali dovrebbero essere in ogni caso concise e trasparenti e in una forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

91. L'EDPB ricorda che il semplice uso della parola "pubblicità" non sarebbe sufficiente per informare gli utenti in merito al fatto che la loro attività viene monitorata per finalità di pubblicità mirata. Dovrebbe essere comunicato in modo trasparente alle persone fisiche quali tipi di trattamento vengono effettuati e che cosa comportino concretamente per l'interessato. Gli interessati dovrebbero essere informati in un linguaggio facilmente comprensibile dell'eventualità che venga definito un profilo sulla base del loro comportamento online sulla piattaforma o sul sito web del *targeter* rispettivamente da parte della piattaforma sociale e del *targeter*, nonché sulle categorie di dati personali raccolti per creare tali profili e, in ultima analisi, per consentire il *targeting* e la pubblicità comportamentale da parte dei *targeter*[90]. Gli utenti dovrebbero ricevere le informazioni pertinenti direttamente sullo schermo, in modo interattivo e, se appropriato o necessario, attraverso informative multilivello[91].

6.1 CONTENUTO ESSENZIALE DELL'ACCORDO E INFORMAZIONI DA FORNIRE (ARTICOLO 26, PARAGRAFO 2, GDPR)

92. Conformemente all'articolo 26, paragrafo 1, GDPR, i contitolari del trattamento *"determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati"*.

93. Un'ulteriore espressione del principio di trasparenza è l'obbligo di mettere a disposizione dell'interessato il contenuto essenziale dell'accordo di contitolarità conformemente all'articolo 26, paragrafo 2, del GDPR. In effetti l'articolo 26 GDPR richiede ai contitolari del trattamento di adottare misure appropriate per garantire che gli interessati siano informati della distribuzione delle responsabilità.

94. In linea di principio l'informazione fornita all'interessato deve riguardare tutti gli aspetti del trattamento o dei trattamenti per i quali i contitolari del trattamento sono congiuntamente responsabili. In effetti l'interessato ha il diritto di ricevere tutte le informazioni (anche per quanto riguarda il trattamento successivo previsto in caso di contitolarità) in via preliminare, in modo che l'informazione sia corretta e adeguata. Più precisamente tale accordo di contitolarità deve assicurare che l'interessato riceva le informazioni richieste dagli articoli 13 e 14 GDPR, anche sulle finalità condivise o stretta-

mente collegate, sui periodi di conservazione, sulla trasmissione a terzi, ecc., che devono essere comunicate all'interessato al momento della raccolta dei dati o prima dell'inizio del trattamento. L'accordo deve chiarire a chi spettano le responsabilità a questo proposito. Per soddisfare tali prescrizioni, detto accordo deve contenere (o fare riferimento a) informazioni chiare ed esaurienti riguardo al trattamento a cui si riferisce con spiegazioni, se del caso, sulle varie fasi del trattamento e sui vari soggetti coinvolti nello stesso[92].

95. Pur essendo entrambi tenuti a fornire informazioni in presenza di una responsabilità congiunta, i contitolari del trattamento possono concordare che uno di loro sia incaricato di fornire le informazioni iniziali agli interessati, in particolare nei casi in cui soltanto uno di essi interagisce con gli utenti prima del trattamento, ad esempio sul proprio sito web[93]. Tale scambio di informazioni da fornire all'interessato dovrebbe essere parte integrante dell'accordo di contitolarità (ad esempio in un'appendice). Nel caso in cui uno dei contitolari del trattamento non disponga di tutte le informazioni in dettaglio poiché, ad esempio, non conosce l'esatta esecuzione tecnica delle attività di trattamento, l'altro contitolare del trattamento gli metterà a disposizione tutte le informazioni necessarie per consentirgli di fornire all'interessato informazioni complete ai sensi degli articoli 13 e 14 GDPR.

96. L'EDPB rileva che i titolari del trattamento non sono direttamente responsabili di fornire le informazioni richieste dagli articoli 13 e 14 GDPR in relazione a ulteriori trattamenti che non rientrano nell'ambito della contitolarità di trattamento. Per questo motivo il *targeter* non è direttamente responsabile di fornire le informazioni relative a qualsiasi ulteriore trattamento che sarà effettuato dalla piattaforma di social media[94].

97. Tuttavia l'EDPB sottolinea che il contitolare del trattamento che intende utilizzare ulteriormente i dati personali è soggetto agli obblighi specifici di informazione in relazione a tale ulteriore trattamento laddove non vi sia responsabilità congiunta, conformemente all'articolo 14, paragrafo 4, GDPR, così come agli obblighi di verificare la compatibilità dell'ulteriore trattamento ai sensi dell'articolo 6, paragrafo 4. Ad esempio il *targeter* e il fornitore di social media potrebbero concordare che il *targeter* fornirà alcune informazioni per conto del fornitore di social media. Tuttavia, il fornitore di social media ha in ultima analisi la responsabilità di garantire che l'interessato abbia ricevuto le informazioni pertinenti in relazione a tutte le attività di trattamento soggette al suo controllo.

Nell'esempio 3 (signor Lopez oggetto di attività di *targeting* in relazione alla pubblicità della banca X sulla sua pagina di social media dopo che la banca ha caricato il suo indirizzo di posta elettronica sulla piattaforma del fornitore di social media), la banca deve informare il signor Lopez in merito al fatto che il suo indirizzo di posta elettronica sarà utilizzato per fini di pubblicità, tramite il fornitore di social media, di offerte legate ai servizi della banca. Qualsiasi ulteriore trattamento da parte del fornitore di social media deve essere lecito e compatibile con le finalità per le quali

la banca ha raccolto i dati.

Nella misura in cui intende trattare ulteriormente l'indirizzo di posta elettronica del signor Lopez per una finalità diversa, il fornitore di social media deve inoltre assicurarsi che il signor Lopez riceva le informazioni richieste dall'articolo 14, paragrafo 4, GDPR prima di procedere in tal senso.

Il fornitore di social media e la banca possono concordare che quest'ultima fornisca al signor Lopez le informazioni pertinenti per conto del fornitore di social media. Anche in tal caso il fornitore di social media ha comunque, in ultima analisi, la responsabilità di garantire che l'interessato abbia ricevuto le informazioni pertinenti in relazione a tutte le attività di trattamento delle quali il fornitore è (il solo) responsabile. Tale obbligo non si applicherebbe qualora il signor Lopez fosse già stato informato dalla banca in merito a tale trattamento, conformemente all'articolo 14, paragrafo 5, lettera a), GDPR.

Tali obblighi di trasparenza devono essere tenuti in conto senza pregiudizio degli obblighi specifici applicabili con riguardo alla base giuridica.

98. A ciascun contitolare del trattamento spetta la responsabilità di assicurare che il contenuto essenziale dell'accordo sia messo a disposizione dell'interessato. In pratica il contenuto essenziale dell'accordo dovrebbe essere disponibile direttamente sulla piattaforma, menzionato nella privacy policy di quest'ultima nonché reso direttamente accessibile attraverso un collegamento ipertestuale, ad esempio nella pagina del *targeter* sulla piattaforma di social media o tramite collegamenti ipertestuali del tipo "perché questo annuncio?".

6.2 DIRITTO DI ACCESSO (ARTICOLO 15)

99. I titolari del trattamento devono consentire agli utenti di esercitare facilmente e pienamente i diritti spettanti agli interessati. L'interessato dovrebbe disporre di uno strumento di facile utilizzo ed efficiente per garantire l' esercizio di tutti i suoi diritti, in qualsiasi momento, in particolare il diritto di cancellazione, di opposizione e il diritto di accesso ai sensi dell'articolo 15 GDPR[95]. I paragrafi che seguono si concentrano sulle modalità di esercizio del diritto di accesso e sui soggetti responsabili di garantire tale esercizio nel contesto del *targeting* degli utenti di social media[96].

100. In via generale, al fine di adempiere le prescrizioni di cui all'articolo 15, paragrafo 1, GDPR e di assicurare piena trasparenza, i titolari del trattamento potrebbero prendere in considerazione un meccanismo che consenta agli interessati di verificare il proprio profilo, nonché i dettagli delle informazioni e delle fonti utilizzate per crearlo. L'interessato dovrebbe poter conoscere l'identità del *targeter* e i titolari del trattamento dovrebbero facilita-

re l'accesso alle informazioni riguardanti il *targeting*, compresi i criteri di *targeting* che sono stati utilizzati, così come le altre informazioni richieste dall'articolo 15 GDPR[97].

101. Per quanto concerne il tipo di accesso da fornire agli interessati, il considerando 63 specifica altresì che *"ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali"*. Le caratteristiche specifiche dei fornitori di social media (contesto online, esistenza di un account utente) suggeriscono la possibilità di permettere facilmente all'interessato l'accesso remoto ai dati personali che lo riguardano conformemente all'articolo 15, paragrafi 1 e 2, GDPR. L'accesso remoto in questo caso può essere considerato come la "misura" più "appropriata" ai sensi dell'articolo 12, paragrafo 1, GDPR, tenendo anche conto del fatto che si tratta di una situazione tipica "in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online" (cfr. considerando 58, che aggiunge esplicitamente la "pubblicità online" come esempio concreto). Inoltre, laddove richiesto, gli utenti di social media oggetto di attività di *targeting* dovrebbero altresì ricevere una copia dei dati personali che li riguardano conformemente all'articolo 15, paragrafo 3, GDPR.

102. Conformemente all'articolo 15, paragrafo 1, lettera c), GDPR, l'utente deve avere acceso in particolare ad informazioni quali *"i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali"*. Conformemente all'articolo 4, punto 9, il termine "destinatario" fa riferimento alla persona fisica o giuridica, all'autorità pubblica, al servizio o a un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Un *targeter* non sarà necessariamente un "destinatario" dei dati personali (cfr. esempio 1), in quanto i dati personali potrebbero non essergli comunicati, ma riceverà le statistiche dei clienti oggetto di *targeting* in forma aggregata o anonima, ad esempio nel contesto della sua campagna o di un riesame delle prestazioni della stessa. Tuttavia nella misura in cui il *targeter* agisce in veste di contitolare del trattamento, deve essere identificato come tale all'utente di social media.

103. Sebbene l'articolo 15 GDPR non sia esplicitamente menzionato nell'articolo 26, paragrafo 1, GDPR, la formulazione di tale articolo fa riferimento a tutte le "responsabilità in merito all'osservanza" degli obblighi derivanti dal GDPR, nei quali rientra l'articolo 15 GDPR.

104. Al fine di consentire agli interessati di esercitare i loro diritti in maniera efficace e facilmente accessibile, l'accordo tra il fornitore di social media e il *targeter* può designare un punto unico di contatto per gli interessati. I contitolari del trattamento sono in linea di principio liberi di determinare chi tra loro dovrebbe essere incaricato di rispondere a e soddisfare le richieste degli interessati, ma non possono escludere la possibilità per l'interessato di esercitare i suoi diritti nei confronti di ciascuno di essi (articolo 26,

paragrafo 3, GDPR). Di conseguenza i *targeter* e i fornitori di social media devono garantire che sia in essere un meccanismo adeguato per consentire agli interessati di ottenere con facilità l'accesso ai propri dati personali (compresi i criteri di *targeting* utilizzati) così come a tutte le informazioni richieste dall'articolo 15 GDPR.

7. VALUTAZIONI D'IMPATTO SULLA PROTEZIONE DEI DATI

105. In linea di principio, prima di avviare le operazioni di *targeting* previste, entrambi i contitolari del trattamento dovrebbero verificare l'elenco dei trattamenti "che possono presentare un rischio elevato" adottato a livello nazionale ai sensi dell'articolo 35, paragrafo 4, e dei considerando 71, 75 e 91 GDPR per determinare se il *targeting* designato corrisponde a uno dei tipi di trattamento soggetti all'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati. Per valutare se le operazioni di *targeting* previste "possono presentare un rischio elevato" e se è necessaria una valutazione d'impatto sulla protezione dei dati, si dovrebbero prendere in considerazione anche i criteri individuati nelle linee guida su tale valutazione[98], nonché gli elenchi stabiliti dalle autorità di controllo relativamente ai trattamenti che sono soggetti all'obbligo di una valutazione d'impatto sulla protezione dei dati (ai sensi dell'articolo 35, paragrafo 4).

106. In taluni casi la natura del prodotto o del servizio pubblicizzato, il contenuto del messaggio o il modo in cui la pubblicità viene trasmessa potrebbero produrre effetti sulle persone fisiche, e tale impatto deve essere ulteriormente valutato. Ciò potrebbe essere il caso ad esempio di prodotti che si rivolgono a persone vulnerabili. Ulteriori rischi possono emergere a seconda delle finalità della campagna pubblicitaria e della sua invasività oppure qualora il *targeting* comporti il trattamento di dati personali osservati, desunti o derivati.

107. Oltre agli obblighi specificamente menzionati nell'articolo 26, paragrafo 1, GDPR, i contitolari del trattamento dovrebbero considerare anche altri elementi nel determinare i loro rispettivi obblighi. Come indicato nelle linee guida dell'EDPB sulle valutazioni d'impatto sulla protezione dei dati "Qualora il trattamento coinvolga contitolari del trattamento, questi ultimi devono definire con precisione le rispettive competenze".

108. Di conseguenza entrambi i contitolari del trattamento devono valutare se sia necessaria una valutazione d'impatto sulla protezione dei dati. Laddove tale valutazione sia necessaria, sono entrambi responsabili dell'adempimento di tale obbligo. L'EDPB ricorda che la valutazione d'impatto sulla protezione dei dati dovrebbe riguardare il trattamento di dati personali nella sua interezza, il che significa che in linea di principio entrambi i contitolari del trattamento devono prendere parte alla realizzazione di tale valutazione. In tale contesto entrambi i titolari del trattamento devono assicurarsi di disporre di un livello sufficiente di informazioni sul trattamento per effettuare la valutazione d'impatto sulla protezione dei dati richiesta[99]. Ciò

implica che "[c]iascun titolare del trattamento deve esprimere le proprie esigenze e condividere informazioni utili senza compromettere eventuali segreti (ad esempio protezione di segreti aziendali, proprietà intellettuale, informazioni aziendali riservate) o divulgare vulnerabilità"[100].

109. In pratica i contitolari del trattamento possono stabilire che spetti a uno di loro eseguire la valutazione d'impatto sulla protezione dei dati. Ciò dovrebbe poi essere specificato nell'accordo di contitolarità, facendo salva la responsabilità congiunta dei titolari in quanto tale. Può darsi che uno dei titolari del trattamento si trovi in una posizione migliore per valutare determinati trattamenti. Ad esempio tale titolare del trattamento può essere, a seconda del contesto, quello che dispone del grado di controllo e di conoscenze più elevato in merito al trattamento di *targeting* - in particolare sul back-end del sistema distribuito o sui mezzi di trattamento.

110. Ogni valutazione d'impatto sulla protezione dei dati deve comprendere le misure previste per affrontare i rischi, fra cui le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione. Se i rischi individuati non possono essere attenuati in misura sufficiente (ossia, se i rischi residui rimangono elevati), i contitolari del trattamento sono responsabili, ciascuno per la propria parte, di assicurare che vengano consultate in via preventiva le autorità di controllo competenti. Qualora violi il GDPR, in particolare perché i rischi non sono stati identificati o attenuati sufficientemente, il *targeting* non dovrebbe avere luogo.

Esempio 9

Il partito politico "Cambiamoilmondo" intende incoraggiare gli utenti di social media a votare per un particolare candidato politico alle successive elezioni. Desidera rivolgersi in maniera mirata a persone anziane che vivono in zone rurali del paese, che si recano regolarmente in chiesa e che non hanno viaggiato all'estero negli ultimi 2 anni.

111. Esiste una contitolarità tra la piattaforma di social media e il partito politico, per l'abbinamento del profilo e la visualizzazione della pubblicità mirata. L'esame della necessità di effettuare una valutazione d'impatto sulla protezione dei dati va svolto tanto dal partito politico Cambiamoilmondo quanto dalla piattaforma di social media. In effetti, in questo esempio, entrambi dispongono di una conoscenza sufficiente dei criteri che vengono utilizzati per rivolgersi in maniera mirata alle persone fisiche così da constatare che il trattamento può presentare un rischio elevato.

112. Qualora sia necessaria una valutazione d'impatto sulla protezione dei dati, l'accordo di contitolarità dovrebbe disciplinare le modalità di svolgimento della stessa da parte dei titolari del trattamento e assicurare che avvenga un pertinente scambio di conoscenze. In questo esempio può essere che la

piattaforma di social media si trovi in una posizione migliore per valutare determinati trattamenti, nella misura in cui il partito politico si limiti a selezionare criteri generali di *targeting*.

8. CATEGORIE PARTICOLARI DI DATI

8.1 CHE COSA COSTITUISCE UNA CATEGORIA PARTICOLARE DI DATI

113. Il GDPR prevede una protezione specifica per i dati personali che sono particolarmente sensibili in relazione ai diritti e alle libertà fondamentali delle persone. Tali dati sono definiti nell'articolo 9 GDPR come categorie particolari di dati personali e comprendono i dati sulla salute, sull'origine razziale o etnica, sulla biometria, sulle convinzioni religiose o filosofiche, sulle opinioni politiche, sull'appartenenza sindacale, sulla vita sessuale o sull'orientamento sessuale di una persona.

114. I titolari del trattamento possono trattare categorie particolari di dati soltanto se sono in grado di soddisfare una delle condizioni di cui all'articolo 9, paragrafo 2, GDPR, quali l'aver ottenuto il consenso esplicito dell'interessato oppure il fatto che i dati siano stati resi manifestamente pubblici dall'interessato. Oltre alle condizioni dell'articolo 9 GDPR, il trattamento di categorie particolari di dati deve fondarsi su una base giuridica stabilita nell'articolo 6 GDPR ed essere effettuato in conformità con i principi fondamentali di cui all'articolo 5 GDPR.

115. Inoltre il trattamento di categorie particolari di dati personali è un elemento pertinente ai fini della valutazione delle misure appropriate secondo gli articoli 24, 25, 28 e 32 GDPR, ma anche per stabilire la necessità o meno di effettuare una valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 GDPR nonché l'opportunità o meno di nominare un responsabile della protezione dei dati a norma dell'articolo 37 GDPR.

116. Nel contesto dei social media e del *targeting*, è necessario stabilire se il trattamento dei dati personali concerne "categorie particolari di dati" e se tali dati sono trattati dal fornitore di social media, dal *targeter* o da entrambi. Se vengono trattate categorie particolari di dati personali, occorre stabilire se e a quali condizioni il fornitore di social media e il *targeter* possono trattare lecitamente tali dati.

117. Se tratta una categoria particolare di dati per finalità di *targeting*, il fornitore di social media deve individuare una base giuridica per il trattamento di cui all'articolo 6 GDPR e fare affidamento su una delle deroghe di cui all'articolo 9, paragrafo 2, GDPR, per esempio il consenso esplicito a norma dell'articolo 9, paragrafo 2, lettera a), GDPR. Se un *targeter* coinvolge un fornitore di social media e chiede a quest'ultimo di rivolgersi in maniera mirata agli utenti sulla base di tale categoria particolare di dati, il *targeter* sarà responsabile congiuntamente al fornitore di social media del trattamento dei dati appartenenti a tale categoria particolare.

118. L'analisi giuridica che segue esaminerà diverse situazioni nelle quali tale trattamento può avere luogo e le rispettive implicazioni.

8.1.1 APPARTENENZA ESPLICITA DI UN DATO A UNA CATEGORIA PARTICOLARE

119. In alcune situazioni i dati personali trattati rientrano chiaramente nella definizione di categorie particolari di dati, ad esempio nel caso di una dichiarazione esplicita in merito all'appartenenza a un determinato partito politico o a una specifica associazione religiosa.

> Esempio 10
>
> La signora Flora dichiara esplicitamente nel proprio profilo sui social media di essere membro del partito politico PianetaPiùVerde. L'organizzazione ambientalista "Lunga vita alla Terra" intende rivolgersi in maniera mirata agli utenti di social media che sono membri del partito politico PianetaPiùVerde per rivolgere loro messaggi mirati.

120. Nell'esempio 10 il fornitore di social media e l'organizzazione ambientalista agiscono in veste di contitolari del trattamento[101]. Nella misura in cui l'organizzazione ambientalista chiede al fornitore di social media di rivolgersi in maniera mirata agli utenti sulla base delle loro opinioni politiche, entrambi i titolari del trattamento contribuiscono al trattamento di categorie particolari di dati come definite dall'articolo 9 GDPR. Il trattamento di tali dati è in linea di principio vietato ai sensi dell'articolo 9, paragrafo 1. Tanto il fornitore di social media quanto l'organizzazione ambientale devono quindi essere in grado di invocare una delle deroghe di cui all'articolo 9, paragrafo 2, per giustificare il loro trattamento. Inoltre devono disporre entrambi di una base giuridica conformemente all'articolo 6. Considerando le deroghe di cui all'articolo 9, paragrafo 2, le uniche applicabili nella situazione di specie risultano essere l'ottenimento del consenso esplicito dell'interessato, ai sensi dell'articolo 9, paragrafo 2, lettera a), GDPR oppure la deroga derivante dal fatto che la signora Flora ha reso manifestamente pubblici i dati personali, ai sensi dell'articolo 9, paragrafo 2, lettera e), GDPR.

8.1.2 APPARTENENZA DI UN DATO A UNA CATEGORIA PARTICOLARE SULLA BASE DI INFERENZE E COMBINAZIONI DI INFORMAZIONI

121. Ipotesi o inferenze riguardanti dati appartenenti a categorie particolari, per cui ad esempio è probabile che una persona voti per un determinato partito dopo aver visitato una pagina che predica opinioni liberali, costituirebbero anch'esse una categoria particolare di dati personali. Analogamente, come già affermato dall'EDPB, *"[l]a profilazione può creare dati appartenenti a categorie particolari desumendoli da dati che di per sé non appartengono a categorie particolari ma che diventano tali se combinati con altri dati. Ad esempio,*

può essere possibile desumere lo stato di salute di una persona associando le registrazioni dei suoi acquisti di alimenti a dati sulla qualità e sul contenuto energetico di tali alimenti"[102].

122. Ad esempio il trattamento di una semplice dichiarazione o di un singolo dato relativo all'ubicazione o analogo, che rivela che un utente ha visitato (una volta o in alcune occasioni) un luogo tipicamente visitato da persone con determinate credenze religiose, non sarà generalmente considerato di per sé un trattamento di categorie particolari di dati. Tuttavia può essere considerato un trattamento di categorie particolari di dati se tali informazioni sono combinate con altri dati oppure in ragione del contesto in cui i dati sono trattati o delle finalità per cui vengono utilizzati.

Esempio 11

Il profilo dell'account del social media del signor Novak rivela soltanto informazioni generali quali il suo nome e il suo domicilio, ma un aggiornamento di stato rivela che ha visitato spesso la Chiesa della Città dove ha partecipato a una funzione religiosa. Successivamente la Chiesa della Città vuole rivolgersi in maniera mirata ai suoi visitatori con messaggi religiosi per incoraggiare i cristiani a unirsi alla congregazione. In tali circostanze l'utilizzo dei dati personali contenuti nell'aggiornamento di stato del signor Novak per tali finalità di *targeting* equivale al trattamento di categorie particolari di dati personali.

123. Se un fornitore di social media o un *targeter* utilizza dati osservati per categorizzare gli utenti in rapporto a determinate credenze religiose, filosofiche o politiche (indipendentemente dal fatto che la categorizzazione sia corretta/vera o meno), tale categorizzazione dell'utente deve ovviamente essere considerata come un trattamento di una categoria particolare di dati personali in questo contesto. Nella misura in cui la categorizzazione consenta il *targeting* basato su dati di categorie particolari, non è importante come sia etichettata tale categoria.

Esempio 12

Il signor Sifuentes fornisce informazioni nel suo profilo del social media sotto forma di aggiornamenti regolari di stato, registrazioni, ecc., che indicano che partecipa regolarmente alle attività organizzate dal "Movimento Mente, Corpo e Spirito". Anche se non viene fornita alcuna dichiarazione esplicita in merito alla credenza filosofica, tutti gli aggiornamenti, i "mi piace", i "registrati" e i dati analoghi forniti dall'utente, se associati tra loro, indicano fortemente che il signor Sifuentes ha un determinato credo filosofico.

Esempio 13

Un fornitore di social media utilizza le informazioni fornite attivamente dalla signora Allgrove sulla pagina del suo profilo di social media sulla sua età, sui suoi interessi e sull'indirizzo e le combina con i dati osservati sui siti web da lei visitati e i suoi "mi piace" sulla piattaforma di social media. Il fornitore di social media utilizza i dati per desumere che la signora Allgrove è una sostenitrice della politica liberale di sinistra e la inserisce nella categoria di *targeting* "interessata alla politica liberale di sinistra" e rende tale categoria disponibile ai *targeter* per la pubblicità mirata.

124. Nell'esempio 12, la mole di informazioni e l'assenza di misure per impedire il *targeting* basato su dati appartenenti a categorie particolari implica che viene effettuato un trattamento di categorie particolari di dati. Tuttavia, il semplice fatto che un fornitore di social media tratti grandi quantità di dati potenzialmente utilizzabili per desumere categorie particolari di dati non significa automaticamente che il trattamento ricada nell'ambito di applicazione dell'articolo 9 GDPR. L'applicazione dell'articolo 9 non ricorre se il trattamento da parte del fornitore di social media non comporta inferenze su categorie particolari di dati e se il fornitore di social media ha adottato misure per evitare che tali inferenze siano possibili o che i dati appartenenti a tali categorie possano essere utilizzati per il *targeting*. In ogni caso il trattamento di un'ampia quantità di dati personali degli utenti può comportare rischi specifici per i diritti e le libertà delle persone fisiche, che devono essere affrontati attuando misure di sicurezza appropriate, come prescritto dall'articolo 32 GDPR e anche tenendo conto del risultato della valutazione d'impatto sulla protezione dei dati da effettuare a norma dell'articolo 35 GDPR.

125. Nell'esempio 13 l'offerta e l'utilizzo della categoria di *targeting* "interessato alla politica liberale di sinistra" equivale al trattamento di categorie particolari di dati, poiché tale categoria potrebbe facilmente essere utilizzata come un utile rimpiazzo al fine di rivolgersi in maniera mirata a persone che hanno convinzioni politiche liberali di sinistra. Assegnando un'opinione politica desunta a un utente, il fornitore di social media tratta categorie particolari di dati. Ai fini dell'articolo 9 GDPR non è rilevante il fatto che l'utente sia effettivamente un sostenitore della politica liberale di sinistra. Né è rilevante che la categoria di *targeting* sia denominata "interessato a…" e non "sostenitore di…", poiché l'utente è inserito nella categoria di *targeting* sulla base di interessi politici desunti.

Esempio 14

Il signor Svenson fa un test attitudinale di carriera, contenente una valutazione psicologica e sviluppato dall'impresa "IlTuoLavoroPerfetto", che è reso disponibile su una piattaforma di social media e fa uso dell'inter-

faccia di programmazione delle applicazioni (API) messa a disposizione del fornitore di social media. IlTuoLavoroPerfetto raccoglie dati sull'istruzione, lo stato di occupazione, l'età, gli hobby, i post, l'indirizzo di posta elettronica e i collegamenti del signor Svenson. IlTuoLavoroPerfetto ottiene i dati attraverso l'API in conformità con le "autorizzazioni" concesse dal signor Svenson attraverso il suo account sui social media. La finalità dichiarata dell'applicazione consiste nel prevedere quale sarebbe il miglior percorso di carriera per un utente specifico.
All'insaputa e senza l'approvazione del fornitore di social media, IlTuoLavoroPerfetto utilizza tali informazioni per desumere una serie di aspetti personali, compresi i tratti della personalità, il profilo psicologico e le convinzioni politiche. IlTuoLavoroPerfetto decide in seguito di utilizzare tali informazioni per rivolgersi in maniera mirata al signor Svenson per conto di un partito politico, utilizzando la funzione di *targeting* basata sugli indirizzi di posta elettronica del fornitore di social media, senza aggiungere altri criteri di *targeting* offerti dal fornitore di social media.

Nell'esempio 14 il *targeter* tratta categorie particolari di dati personali, mentre il fornitore di social media non lo fa. Infatti la valutazione e l'identificazione del credo politico del signor Svenson avviene senza il coinvolgimento del fornitore di social media[103]. Oltre a far scattare il divieto generale dell'articolo 9 GDPR, il *targeting* menzionato nell'esempio 14 costituisce anche una violazione dei requisiti di correttezza, trasparenza e limitazione della finalità. In effetti il signor Svenson non è adeguatamente informato in merito al fatto che i dati personali che lo riguardano saranno trattati per attività di *targeting* politico, circostanza questa che inoltre non sembra compatibile con un test attitudinale di carriera.

126. Mentre le attività di trattamento del fornitore di social media di cui all'esempio 14 non costituiscono un trattamento di categorie particolari di dati ai sensi dell'articolo 9 GDPR, il fornitore di social media è responsabile dell'integrazione delle necessarie garanzie nel trattamento al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati in conformità agli articoli 24 e 25 GDPR.

8.2 L'ECCEZIONE DI CUI ALL'ARTICOLO 9, PARAGRAFO 2 PER CATEGORIE PARTICOLARI DI DATI RESI MANIFESTAMENTE PUBBLICI

127. L'articolo 9, paragrafo 2, lettera e), GDPR consente il trattamento di una categoria particolare di dati nei casi in cui i dati sono stati resi manifestamente pubblici dall'interessato. La parola "manifestamente" implica l'esistenza di una soglia elevata per poter invocare tale deroga. L'EDPB osserva che la presenza di un singolo elemento può non essere sempre sufficiente a stabilire che i dati sono stati "manifestamente" resi pubblici dall'interessato. Nella pratica i titolari del trattamento potrebbero dover considerare una combinazione dei seguenti elementi o di altri elementi per dimostrare che

l'interessato ha manifestato chiaramente l'intenzione di rendere pubblici i dati; inoltre è necessaria una valutazione caso per caso. I seguenti elementi possono essere pertinenti ai fini di tale valutazione:

i) le impostazioni predefinite della piattaforma di social media (ossia l'eventualità che l'interessato abbia intrapreso un'azione specifica per modificare tali impostazioni predefinite come private in pubbliche); oppure

ii) la natura della piattaforma di social media (ossia se la piattaforma in questione è intrinsecamente legata all'idea di creare legami con conoscenti stretti dell'interessato o di creare relazioni intime (come le piattaforme di incontri online) oppure è destinata a fornire un ambito più ampio di relazioni interpersonali, quali relazioni professionali o microblogging, la condivisione di media, le piattaforme sociali per condividere recensioni online, ecc.); oppure

iii) l'accessibilità della pagina dove sono pubblicati i dati sensibili (ossia se le informazioni sono accessibili pubblicamente o se, ad esempio, è necessaria la creazione di un account prima di accedere alle informazioni); oppure

iv) la visibilità dell'informazione quando l'interessato è informato della natura pubblica delle informazioni che sta postando (ossia se c'è ad esempio un banner continuo sulla pagina o se il pulsante di pubblicazione informa l'interessato che l'informazione sarà resa pubblica...); oppure

v) se l'interessato ha pubblicato personalmente i dati sensibili o se invece i dati sono stati pubblicati da un terzo (ad esempio una foto pubblicata da un amico che rivela dati sensibili) o sono stati desunti.

128. L'EDPB osserva che la presenza di un singolo elemento può non essere sempre sufficiente a stabilire che i dati sono stati "manifestamente" resi pubblici dall'interessato. Nella pratica i titolari del trattamento potrebbero dover considerare una combinazione di questi o di altri elementi per dimostrare che l'interessato ha manifestato chiaramente l'intenzione di rendere pubblici i dati.

Esempio 15

Il signor Jansen ha aperto un account su una piattaforma di social media di microblogging. Mentre completava il proprio profilo ha indicato di essere omosessuale. Essendo un conservatore, ha scelto di unirsi a gruppi conservatori sapendo, essendone stato informato durante l'iscrizione, che i messaggi che scambia sulla piattaforma sono pubblici. Un partito politico conservatore desidera rivolgersi in maniera mirata a persone che condividono la stessa affiliazione politica e lo stesso orientamento sessuale del signor Jansen utilizzando strumenti di *targeting* tramite social media.

129. Dato che l'orientamento sessuale dei membri è per impostazione predefinita "privato" e che il signor Jansen non ha compiuto alcuna azione per

renderlo pubblico, non si può considerare che tale informazione sia stata manifestamente resa pubblica. Inoltre i dati relativi alla sua affiliazione politica non sono stati resi manifestamente pubblici, nonostante i) la natura della piattaforma di social media di microblogging, che è destinata a condividere informazioni con il vasto pubblico e ii) il fatto che sia stato informato del carattere pubblico dei messaggi che pubblica sui forum. Inoltre, anche se ha aderito a forum pubblici relativi al conservatorismo, non è possibile rivolgersi a lui in maniera mirata sulla base di tali dati sensibili, dato che è la piattaforma di social media che effettua una deduzione sull'affiliazione politica del signor Janssen e non era intenzione specifica dell'interessato rendere tali dati manifestamente pubblici, tanto più che questa deduzione può rivelarsi falsa. Non è quindi possibile rivolgersi a lui in maniera mirata sulla base di dati di affiliazione politica. In altre parole occorre prendere in considerazione le circostanze di ciascun caso specifico al fine di valutare se i dati sono stati manifestamente resi pubblici dall'interessato[104].

9. CONTITOLARITÀ E RESPONSABILITÀ CONGIUNTA

9.1 ACCORDO TRA I CONTITOLARI DEL TRATTAMENTO E DETERMINAZIONE DELLE RESPONSABILITÀ (ARTICOLO 26 GDPR)

130. L'articolo 26, paragrafo 1, GDPR impone ai contitolari del trattamento di determinare in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, come spiegato sopra, anche per quanto concerne gli obblighi di trasparenza.

131. In termini di ambito di applicazione, l'EDPB ritiene che l'accordo tra i *targeter* e i fornitori di social media dovrebbe comprendere tutti i trattamenti per i quali essi sono congiuntamente responsabili (ossia soggetti alla loro contitolarità). Qualora concludessero un accordo avente natura meramente superficiale nonché incompleto, i *targeter* e i fornitori di social media sarebbero in violazione dei loro obblighi ai sensi dell'articolo 26 GDPR.

> Nell'esempio 4 l'accordo dovrebbe ad esempio coprire l'intero ambito del trattamento di dati personali effettuato in contitolarità, ossia dalla raccolta dei dati personali nell'ambito della visita da parte del signor Schmidt del sito web "MiglioriBorse.com" con un pixel di tracciamento, fino alla visualizzazione della pubblicità sulla sua pagina di social media, nonché all'eventuale rendicontazione relativa alla campagna di *targeting*.

132. Al fine di redigere un accordo completo, tanto il fornitore di social media quanto il *targeter* devono conoscere e disporre di informazioni sufficientemente dettagliate sugli specifici trattamenti di dati che hanno luogo. L'accordo tra il *targeter* e il fornitore di social media dovrebbe quindi contenere (o fare riferimento a) tutte le informazioni necessarie per consentire a

entrambe le parti di rispettare gli obblighi ai sensi del GDPR, compreso il dovere di rispettare i principi di cui all'articolo 5, paragrafo 1, GDPR e di dimostrare la loro conformità ai sensi dell'articolo 5, paragrafo 2, GDPR.

133. Se, ad esempio, il titolare del trattamento pensa di utilizzare l'articolo 6, paragrafo 1, lettera f), GDPR come base giuridica, è necessario, tra l'altro, conoscere l'ambito di applicazione del trattamento dei dati per poter valutare se l'interesse del titolare del trattamento prevalga sugli interessi o sui diritti e sulle libertà fondamentali degli interessati. In assenza di informazioni sufficienti sul trattamento, non è possibile effettuare tale valutazione. Non può sfuggire l'importanza di comprendere o fare riferimento alle informazioni necessarie nel contesto di un accordo di contitolarità, in particolare qualora una delle parti disponga in via pressoché esclusiva della conoscenza e dell'accesso alle informazioni delle quali entrambe le parti necessitano per rispettare il GDPR.

> Nell'esempio 1 quando l'impresa X valuta se può invocare l'interesse legittimo come base giuridica per rivolgersi in maniera mirata a uomini di età compresa tra i 30 e i 45 anni e che hanno indicato di essere single, è necessario ad esempio che abbia accesso a informazioni sufficienti sul trattamento effettuato dalla piattaforma di social media, anche per quanto riguarda le misure aggiuntive (quali il diritto all'opposizione preventiva) messe in atto da quest'ultima per accertare che sugli interessi legittimi non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

134. Al fine di garantire che i diritti dell'interessato possano essere rispettati efficacemente, l'EDPB ritiene che anche la finalità del trattamento e la corrispondente base giuridica dovrebbero riflettersi nell'accordo di contitolarità stipulato tra i *targeter* e i fornitori di social media che sono contitolari del trattamento. Sebbene il GDPR non impedisca ai contitolari del trattamento di utilizzare basi giuridiche diverse per i diversi trattamenti che effettuano, si raccomanda di utilizzare, ove possibile, la medesima base giuridica per un particolare strumento di *targeting* e per una finalità specifica. In effetti, qualora ogni fase del trattamento si fondasse su una base giuridica diversa, ciò renderebbe impraticabile l'esercizio dei diritti per l'interessato (ad esempio per una fase ci sarebbe il diritto alla portabilità dei dati, per un'altra il diritto di opposizione).

135. In qualità di titolari del trattamento, il *targeter* e il fornitore di social media sono entrambi responsabili di assicurare il rispetto del principio di limitazione della finalità e dovrebbero quindi integrare disposizioni appropriate a tal fine nell'accordo di contitolarità.

> Ad esempio se desidera utilizzare i dati personali che gli sono stati forniti dall'interessato al fine di rivolgersi in maniera mirata a quest'ultimo sui social media, il *targeter* deve adottare misure adeguate per garantire che i dati forniti non siano ulteriormente utilizzati dal fornitore di social media

media in modo incompatibile con tali finalità, fatto salvo il caso in cui abbia ottenuto il consenso valido dell'interessato ai sensi dell'articolo 6, paragrafo 4, GDPR.
Nell'esempio 3 la banca X dovrebbe assicurarsi che nell'accordo di contitolarità stipulato con la piattaforma di social media vi siano disposizioni appropriate che assicurino che l'indirizzo di posta elettronica del signor Lopez non sia utilizzato, senza il consenso dello stesso, per altre finalità diverse dalla pubblicità di offerte legate ai servizi bancari che egli sta già utilizzando.
Analogamente il fornitore di social media deve garantire che l'uso dei dati per finalità di *targeting* da parte dei *targeter* sia conforme ai principi di limitazione della finalità, trasparenza e legalità.

136. Altri obblighi che dovrebbero essere considerati dal *targeter* e dal fornitore di social media nel contesto del loro accordo di contitolarità comprendono: altri principi generali in materia di protezione dei dati di cui all'articolo 5 GDPR, la sicurezza del trattamento, la protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, le notifiche e le comunicazioni di violazioni dei dati personali, le valutazioni d'impatto sulla protezione dei dati, l'uso di responsabili del trattamento e i trasferimenti verso paesi terzi.

Nell'esempio 13, qualora sia necessaria una valutazione d'impatto sulla protezione dei dati, l'accordo di contitolarità dovrebbe prevedere a quale dei titolari del trattamento spetti svolgerla nonché assicurare che avvenga un pertinente scambio di conoscenze. In altre parole, il partito politico "Cambiamoilmondo" dovrebbe assicurarsi di disporre di un livello sufficiente di informazioni, ad esempio sulle misure di sicurezza messe in atto dalla piattaforma di social media, quando viene effettuata una valutazione d'impatto sulla protezione dei dati.

137. Infine l'accordo di contitolarità stipulato tra il fornitore di social media e il *targeter* deve contenere informazioni specifiche in merito alle modalità concrete con cui saranno soddisfatti gli obblighi del GDPR. Laddove non vi sia chiarezza in merito alle modalità di soddisfacimento di tali obblighi, in particolare in relazione ai diritti degli interessati, si dovrà ritenere che tanto il *targeter* quanto il fornitore di social media stiano violando l'articolo 26, paragrafo 1, GDPR. Inoltre in tali casi entrambi i (con)titolari del trattamento non avranno attuato misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento sia stato condotto in conformità con il GDPR, e quindi avranno violato i loro obblighi ai sensi dell'articolo 5, paragrafo 2, e dell'articolo 24.

9.2 LIVELLI DI RESPONSABILITÀ

138. L'EDPB osserva che i *targeter* che desiderano utilizzare gli strumenti di *targeting* messi a disposizione da un fornitore di social media possono trovarsi di fronte alla necessità di aderire ad accordi predefiniti, senza alcuna possibilità di negoziare o apportare modifiche (condizioni "prendere o lasciare"). L'EDPB ritiene che ciò non infici la responsabilità congiunta del fornitore di social media e del *targeter* e non possa esonerare una delle due parti dai suoi obblighi ai sensi del GDPR. Entrambe le parti dell'accordo di contitolarità sono altresì tenute a garantire che l'assegnazione delle responsabilità rifletta debitamente i rispettivi ruoli e le rispettive relazioni nei confronti dei dati degli interessati in modo pratico, veritiero e trasparente.

139. È importante sottolineare che un accordo ai sensi dell'articolo 26 GDPR non può prevalere sugli obblighi giuridici che incombono su un (con)titolare del trattamento. Sebbene, in conformità con l'articolo 26 GDPR, i contitolari del trattamento siano tenuti a "*determina[re] [...] le rispettive responsabilità in merito all'osservanza*" del GDPR, ciascun titolare del trattamento rimane, per principio, responsabile della conformità del trattamento. Ciò significa che ciascun titolare del trattamento è responsabile tra l'altro del rispetto dei principi di cui all'articolo 5, paragrafo 1, GDPR, compreso il principio di liceità di cui all'articolo 5, paragrafo 1, lettera a), GDPR.

140. Tuttavia il grado di responsabilità del *targeter* e del fornitore di social media in relazione agli obblighi specifici può variare. Nella sentenza *Wirtschaftsakademie*, la Corte ha osservato che *"l'esistenza di una responsabilità congiunta non implica necessariamente una responsabilità equivalente, per un medesimo trattamento di dati personali, dei diversi soggetti che vi partecipano. [...] tali soggetti possono essere coinvolti in fasi diverse di tale trattamento e a diversi livelli, di modo che il grado di responsabilità di ciascuno di essi deve essere valutato tenendo conto di tutte le circostanze rilevanti del caso di specie"*[105].

141. In altre parole anche se i contitolari sono entrambi responsabili del rispetto degli obblighi previsti dal GDPR e anche se l'interessato può esercitare i suoi diritti nei confronti di ciascuno dei titolari del trattamento, il loro livello di responsabilità deve essere valutato in base al ruolo effettivo svolto nel trattamento. Nella sentenza *Google Spain*, la Corte ha chiarito che un titolare del trattamento deve assicurare, *"nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità"*, che il trattamento dei dati personali soddisfi le prescrizioni della normativa UE in materia di protezione dei dati[106].

142. Quando si tratta di valutare il livello di responsabilità di *targeter* e fornitori di social media, possono rilevare diversi fattori quali la capacità di influire concretamente sul trattamento, così come la conoscenza effettiva o costruttiva di ciascuno dei contitolari del trattamento. È importante altresì che sia chiaro in quale fase del trattamento e in quale misura o grado il *targeter* e il fornitore di social media siano responsabili per il trattamento[107].

Nell'esempio 1 l'impresa X definisce una campagna pubblicitaria affinché agli utenti corrispondenti a specifici criteri di *targeting* possa essere mostrata pubblicità dell'impresa sulla piattaforma di social media. Tuttavia, sebbene stabilisca i parametri della campagna pubblicitaria, l'impresa non raccoglie né ha accesso ad alcun dato personale, né ha alcun contatto diretto con l'interessato. Ognuno di questi elementi può essere rilevante ai fini della valutazione del livello (o "grado") di responsabilità del *targeter* e del fornitore di social media nel caso in cui venga constatata una violazione del GDPR (ad esempio in caso di mancanza di trasparenza nei confronti dell'interessato o della mancata garanzia della liceità del trattamento). Come indicato in precedenza, nonostante ciò, entrambe le parti sono tenute ad adottare misure appropriate al fine di soddisfare i requisiti del GDPR e proteggere i diritti degli interessati da forme illecite di trattamento.

Nell'esempio 3, che riguardava il *targeting* basato su elenchi, la situazione è leggermente diversa dall'esempio 1. Nell'esempio 3 la banca ha inizialmente raccolto i dati personali e li ha condivisi con il fornitore di social media per finalità di *targeting*. In questo caso il *targeter* ha attivato volontariamente la fase di raccolta e trasmissione dei dati . Ognuno di questi elementi dovrebbe essere preso in considerazione ai fini della valutazione del livello di responsabilità di ciascun soggetto coinvolto e dovrebbe essere debitamente riflesso nelle clausole dell'accordo di contitolarità.

Analogamente, nell'esempio 4, in caso di *targeting* basato su pixel, occorre tenere conto del fatto che il gestore del sito web consente la trasmissione di dati personali al fornitore di social media. È infatti il sito "MiglioriBorse.com" che integra un pixel di tracciamento sul proprio sito web in maniera da potersi rivolgere in maniera mirata al signor Schmidt, anche se quest'ultimo ha deciso di non effettuare un acquisto[108]. Il sito web è quindi attivamente coinvolto nella raccolta e nella trasmissione dei dati. In veste di contitolare del trattamento il fornitore di social media ha tuttavia altresì l'obbligo di adottare misure appropriate per soddisfare i requisiti del GDPR e proteggere i diritti degli interessati da forme illecite di trattamento. In questo caso, laddove venga richiesto il consenso dell'interessato, i contitolari del trattamento devono accordarsi in merito alle concrete modalità di raccolta di tale consenso.

143. Quando si tratta di valutare il livello di responsabilità del fornitore di social media, l'EDPB osserva che diversi meccanismi di *targeting* si basano sulla profilazione e/o su altre attività di trattamento precedentemente intraprese dal fornitore di social media. È il fornitore di social media che decide di trattare i dati personali dei suoi utenti in modo tale da sviluppare i criteri di *targeting* che mette a disposizione dei *targeter*. Per fare ciò il fornitore

di social media ha preso autonomamente alcune decisioni relative al trattamento, come ad esempio quali categorie di dati saranno trattate, quali criteri di *targeting* saranno offerti e chi avrà accesso a (quali tipi di) dati personali trattati nel contesto di una particolare campagna di *targeting*. Tali attività di trattamento devono anche essere conformi al GDPR, prima dell'offerta di qualsiasi servizio di *targeting*.

144. Gli esempi citati nei paragrafi che precedono sottolineano l'importanza di una chiara allocazione di responsabilità nell'accordo di contitolarità stipulato tra i fornitori di social media e i *targeter*. Anche se i termini dell'accordo dovrebbero in ogni caso rispecchiare il livello di responsabilità di ciascun soggetto, un accordo completo che rifletta debitamente il ruolo e le capacità di ogni parte è necessario non soltanto per rispettare l'articolo 26 GDPR, ma anche per rispettare altre norme e altri principi del GDPR.

145. Infine l'EDPB osserva che nella misura in cui i termini dell'accordo di contitolarità stipulato tra il fornitore di social media e il *targeter* non vincolano le autorità di controllo, queste ultime possono esercitare le loro competenze e i loro poteri in relazione a ciascuno dei contitolari del trattamento, nella misura in cui il contitolare del trattamento in questione è soggetto alla competenza di tale autorità di controllo.

NOTE

[1] Le funzioni aggiuntive fornite dai social media possono comprendere ad esempio la personalizzazione, l'integrazione di applicazioni, i plug-in sociali, l'autenticazione dell'utente, l'analisi e la pubblicazione. Le funzioni dei social media possono costituire un'offerta autonoma dei titolari del trattamento oppure possono essere integrate come parte di un'offerta di servizi più ampia.

[2] Oltre alle piattaforme di social media "tradizionali", tra gli ulteriori esempi di social media si annoverano: piattaforme di incontri nel contesto delle quali gli utenti registrati si presentano per trovare partner con cui uscire nella vita reale; piattaforme nel contesto delle quali gli utenti registrati possono caricare i propri video, commentare i video pubblicati da altri e creare collegamenti con tali video; oppure giochi per computer nel contesto dei quali gli utenti registrati possono giocare insieme in gruppi, scambiarsi informazioni o condividere le loro esperienze e i loro successi all'interno del gioco.

[3] Il *targeting* è stato definito come "l'atto di indirizzare o rivolgere qualcosa a un particolare gruppo di persone" nonché come "l'atto di tentare di attrarre una persona o un gruppo o di influenzarli in qualche modo". https://www.collinsdictionary.com/it/dizionario/inglese/targeting.

[4] I messaggi consistono tipicamente in immagini e testo, ma possono anche comprendere formati video e/o audio.

[5] I dati personali trattati nel contesto dei social media possono costituire "categorie particolari di dati personali" ai sensi dell'articolo 9 GDPR, riguardare persone vulnerabili o avere altrimenti una natura estremamente personale. Cfr. altresì Gruppo di lavoro Articolo 29, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, WP 248 rev. 01, pag. 9.

[6] Cfr. ad esempio: https://edpb.europa.eu/sites/default/files/files/file1/201902_edpb_statementonelections_it.pdf; https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recommendations-and-actions-from-ico-investigation-into-data-analytics-in-political-campaigns/; https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52018DC0638&qid=1551268194885&from=IT; https://www.personuvernd.is/information-in-english/greinar/nr/2880.

[7] Corte di giustizia dell'Unione europea, sentenza del 5 giugno 2018 nella causa Wirtschaftsakademie, C-210/16, ECLI:EU:C:2018:388; Corte di giustizia dell'Unione europea, sentenza del 29 luglio 2019 nella causa Fashion ID, C 40/17, ECLI:EU:C:2019:629.

[8] Le presenti linee guida lasciano impregiudicati i contenuti del documento dell'EDPB *Guidelines 07/2020 on the concepts of controller and processor under the GDPR* adottato il 2 settembre 2020, riguardanti la distribuzione delle responsabilità in altri contesti.

[9] Conformemente all'articolo 24 GDPR, il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR, "tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche". Cfr. anche Gruppo di lavoro Articolo 29, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, WP 248 rev. 01, 4 ottobre 2017.

[10] Cfr. anche garante europeo della protezione dei dati (GEPD), parere 3/2018 sulla manipolazione online, 19 marzo 2018, pag. 15 ("*La preoccupazione derivante dall'utilizzo di dati dei profili per finalità diverse attraverso algoritmi è data dal fatto che i dati perdano il loro contesto originale. La ridefinizione delle finalità dei dati può influenzare l'autodeterminazione informativa di una persona, ridurre ulteriormente il controllo degli interessati sui loro dati, influenzando così la fiducia nei confronti dei contesti e dei servizi digitali*").

[11] T. Speicher e a., *Potential for Discrimination in Online Targeted Advertising, Proceedings of the 1st Conference on Fairness, Accountability and Transparency,* Proceedings of Machine Learning Research PMLR 81:5-19, 2018, http://proceedings.mlr.press/v81/speicher18a.html.

[12] Ibidem.

[13] Garante europeo della pro-

tezione dei dati, parere 3/2018, pag. 18.

[14] Cfr. "*Experimental evidence of massive-scale emotional contagion through social networks*", Adam D. I. Kramer, Jamie E. Guillory e Jeffrey T. Hancock, PNAS 17 giugno 2014, 111 (24) 8788-8790; pubblicato per la prima volta il 2 giugno 2014 https://doi.org/10.1073/pnas.1320040111, disponibile all'indirizzo: https://www.pnas.org/content/111/24/8788 Adam D. I. Kramer Core Data Science Team, Facebook, Inc., Menlo Park, CA 94025.

[15] Cfr. anche EDPB, Dichiarazione 2/2019 sull'uso di dati personali nel corso di campagne politiche, 13 marzo 2019, pag. 1

[16] Information Commissioner's Office (ICO), *Democracy disrupted? Personal information and political influence*, 10 luglio 2018, pag. 14.

[17] Cfr. anche Commissione europea, Documento di orientamento, Orientamenti della Commissione sull'applicazione del diritto dell'Unione in materia di protezione dei dati nel contesto elettorale - Contributo della Commissione europea all'incontro dei leader di Salisburgo del 19-20 settembre 2018. Cfr. anche L.M. Neudert e N.M. Marchal, *Polarisation and the use of technology in political campaigns and communication, European Parliamentary Research Service*, 2019, pagg. 22-24.

[18] Cfr. anche risoluzione del Parlamento europeo del 3 maggio 2018 sul pluralismo e la libertà dei media nell'Unione europea.

[19] Garante europeo della protezione dei dati, parere 3/2018, pag. 7.

[20] Garante europeo della protezione dei dati, parere 3/2018, pag. 9 e Comitato di esperti sul pluralismo dei media e la trasparenza della proprietà dei media (MSI-MED), *Internet and Electoral Campaigns, Study on the use of internet in electoral campaigns*, studio del Consiglio d'Europa DGI(2017)11, aprile 2018, pagg. 19-21.

[21] Cfr. anche Gruppo di lavoro Articolo 29, Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, 6 febbraio 2018, WP 251 rev. 01, pag. 29.

[22] https://ec.europa.eu/eurostat /en/web/products-eurostat-news/-/edn-20200630-2.

[23] Dichiarazione del comitato europeo per la protezione dei dati in merito alle ripercussioni delle concentrazioni economiche sulla protezione dei dati, disponibile all'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_it.pdf.

[24] I dati personali e le informazioni di profilazione gestiti dai fornitori di social media in relazione alle persone fisiche che non sono registrate presso i fornitori di social media sono talvolta definiti "profili ombra".

[25] Cfr. anche il considerando 26 ("individuazione"). Cfr. anche Gruppo di lavoro Articolo 29, Parere 4/2007 sul concetto di dati personali, 20 giugno 2007, WP 136, pag. 12 e seguenti.

[26] In alcuni casi i fornitori di social media chiedono ulteriore documentazione per verificare i dati forniti, ad esempio chiedendo agli utenti di caricare le loro carte d'identità o documentazione analoga.

[27] Tale *targeting* può essere reso possibile sulla base di identificatori online forniti dai loro dispositivi, da applicazioni, strumenti e protocolli (quali indirizzi di protocollo internet), identificatori di cookie o altri identificatori. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle. Cfr. anche il considerando 30 GDPR. Sulla base di tale riconoscimento, pubblicità mirate possono essere visualizzate su un sito web che la persona fisica visita.

[28] Il trattamento di dati personali da parte di una persona fisica nel corso di un'attività puramente personale o domestica non rientra nell'ambito di applicazione materiale del GDPR (articolo 2, paragrafo 2, lettera c)).

[29] La semplice condivisione di informazioni su una pagina di social media destinata al grande pubblico (ad esempio, informazioni sugli orari di apertura) senza una preventiva selezione del pubblico destinatario non sarebbe considerata un'attività di "*targeting*" ai fini delle presenti linee guida.

[30] Sulla descrizione dei diversi soggetti coinvolti, cfr. Gruppo di lavoro, Parere 2/2010 sulla pubblicità comportamentale online, pag. 5. Il parere è disponibile all'indirizzo: https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf.

[31] cfr. Consumer Policy Research Centre, "A day in the life of data", disponibile all'indirizzo: http://cprc.org.au/publication/research-report-a-day-in-the-life-of-data/.

[32] Sentenza della Corte di giustizia dell'Unione europea nella causa Wirtschaftsakademie, C-210/16, punto 36.

[33] Sentenza della Corte di giustizia dell'Unione europea nella causa Wirtschaftsakademie, C-210/16, punto 39.

[34] Sentenza della Corte di giu-

stizia dell'Unione europea nella causa Wirtschaftsakademie, C-210/16, punto 43; nonché sentenza nella causa Jehovah's Witnesses, C-25/17, punto 66 e sentenza nella causa Fashion ID, C-40/17, punto 70.

[35] Sentenza della Corte di giustizia dell'Unione europea nella causa Wirtschaftsakademie, C-210/16, punto 30.

[36] Sentenza della Corte di giustizia dell'Unione europea nella causa Fashion ID, C-40/17, punto 75 e seguenti e punto 107.

[37] Sentenza della Corte di giustizia dell'Unione europea nella causa Fashion ID, C-40/17, punto 107.

[38] Il trattamento successivo è qualsiasi operazione o insieme di operazioni di trattamento che segue (ossia ha luogo dopo) la raccolta dei dati. Nella sentenza Fashion ID, il termine è utilizzato per fare riferimento ai trattamenti effettuati da Facebook dopo la loro trasmissione e per i quali Fashion ID non deve essere considerata come un contitolare del trattamento (perché non partecipa effettivamente alla determinazione delle finalità e dei mezzi di tali trattamenti).
L'ulteriore trattamento per una finalità diversa da quella per cui i dati personali sono stati raccolti è ammissibile soltanto nella misura in cui è rispettato l'articolo 6, paragrafo 4, GDPR relativo all'ulteriore trattamento. Ad esempio se un rivenditore online raccoglie i dati relativi all'indirizzo di casa di una persona fisica, un ulteriore trattamento consisterebbe nella conservazione o nella successiva cancellazione di tali informazioni. Tuttavia se tale rivenditore online al dettaglio decidesse in seguito di trattare tali dati personali per arricchire il profilo dell'interessato per finalità di *targeting*, si tratterebbe di un ulteriore trattamento ai sensi dell'articolo 6, paragrafo 4, GDPR, in quanto comporta un trattamento per una finalità diversa da quella per cui sono stati inizialmente raccolti.

[39] Sentenza della Corte di giustizia dell'Unione europea nella causa Fashion ID, C-40/17, punto 76.

[40] Gruppo di lavoro Articolo 29, Linee guida sul diritto alla portabilità dei dati, WP 242 rev. 01, 5 aprile 2017, pag. 11.

[41] Cfr. ad esempio la decisione del Tribunale amministrativo superiore della Baviera h (Germania), Beschluss v.26.9.2018 - 5 CS 18.1157, www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-25018.

[42] Nel suo parere 2/2010 sulla pubblicità comportamentale online il Gruppo di lavoro ha notato che "*vi sono due metodi principali: i) i profili predittivi sono stabiliti per deduzione attraverso l'osservazione del comportamento individuale e collettivo dell'utente nel corso del tempo, in particolare monitorando le pagine visitate e i messaggi pubblicitari visualizzati o cliccati; ii) i profili espliciti sono creati a partire da dati personali che l'interessato stesso ha fornito a un servizio web, per esempio all'atto della registrazione*" (Gruppo di lavoro Articolo 29, Parere 2/2010 sulla pubblicità comportamentale online, WP 171, pag. 8).

[43] Gruppo di lavoro Articolo 29, Linee guida sul diritto alla portabilità dei dati, WP 242 rev. 01, 5 aprile 2017, pag. 11.

[44] *Ibidem.*

[45] Cfr. EDPB, *Linee guida 7/2020 sui concetti di responsabile del trattamento e di titolare del trattamento nel GDPR, ("Inoltre quando le entità non hanno la medesima finalità per il trattamento, la contitolarità può essere stabilita altresì, alla luce della giurisprudenza della Corte di giustizia dell'Unione europea, quando le entità coinvolte perseguono finalità che sono strettamente collegate o complementari. Tale caso può verificarsi ad esempio quando esiste un vantaggio reciproco derivante dal medesimo trattamento, a condizione che ciascuna delle entità coinvolte partecipi alla determinazione delle finalità e dei mezzi del trattamento in questione").*

[46] Cfr. EDPB, *Linee guida 7/2020 sui concetti di responsabile del trattamento e di titolare del trattamento nel GDPR, ("Inoltre la scelta compiuta da un'entità di utilizzare per le proprie finalità uno strumento o un altro sistema sviluppato da un'altra entità, che consente il trattamento dei dati personali, equivarrà probabilmente a una decisione congiunta sui mezzi di tale trattamento da parte di tali entità. Ciò si desume dalla causa Fashion ID nella quale la Corte di giustizia dell'Unione europea ha concluso che incorporando sul proprio sito web il pulsante "Mi piace" di Facebook messo a disposizione dei gestori di siti internet, Fashion ID ha esercitato un'influenza decisiva per quanto riguarda le operazioni di raccolta e trasmissione dei dati personali dei visitatori del suo sito web a Facebook e ha quindi determinato insieme a Facebook le modalità di tale trattamento").*

[47] Cfr. a tale proposito la sentenza della Corte di giustizia dell'Unione europea nella causa Wirtschaftsakademie, C-210/16, ECLI:EU:C:2018:388, punto 39.

[48] Cfr. nella stessa ottica anche la sentenza della Corte di giustizia dell'Unione europea nella causa Fashion ID, C 40/17, punto 80: "*operazioni di trattamento effettuate nell'interesse economico tanto della Fashion ID quanto della Facebook Ireland, per la quale il fatto di poter disporre di tali dati ai propri fini commerciali costituisce la contropartita del vantaggio offerto alla Fashion ID*".

[49] Cfr. parere 1/2010.

[50] Cfr. EDPB, Linee guida 7/2020 sui concetti di responsabile del trattamento e di titolare del trattamento nel GDPR,.

[51] Cfr. anche la sentenza della Corte di giustizia dell'Unione europea nella causa Fashion ID, C-40/17, punto 74 ("*[una] persona fisica o giuridica non può essere considerata responsabile, ai sensi di detta disposizione, delle operazioni anteriori o successive della catena di trattamento di cui essa non determina né le finalità né gli strumenti*") e punto 101.

[52] Sentenza della Corte di giustizia dell'Unione europea nella causa *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, punto 38; sentenza della Corte di giustizia dell'Unione europea nella causa Jehovah's Witnesses, C-25/17, ECLI:EU:C:2018:551, punto 69.

[53] Sentenza della Corte di giustizia dell'Unione europea del 10 luglio 2018 (C 25/17, punti da 68 a 72).

[54] Cfr. punto 18 del documento dell'EDPB, Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, versione 2.0, 8 ottobre 2019, disponibile all'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_it.pdf

[55] Cfr. punti 52 e 53 del documento dell'EDPB, Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, versione 2.0, 8 ottobre 2019, disponibile all'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_it.pdf.

[56] Non sarebbe soddisfatto il criterio della necessità se il *targeter* si servisse dei fornitori di social media pur avendo una relazione contrattuale diretta con il proprio cliente e, quindi, la possibilità di effettuare pubblicità diretta.

[57] Cfr. pag. 17 del documento dell'EDPB, Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, versione 2.0, 8 ottobre 2019, disponibile all'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_it.pdf.

[58] EDPB, Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, punto 57.

[59] Corte di giustizia dell'Unione europea, sentenza del 29 luglio 2019 nella causa Fashion ID, C-40/17, ECLI:EU:C:2019:629, punto 95.

[60] Ibidem, punto 97.

[61] Gruppo di lavoro Articolo 29, Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, WP 217, 9 aprile 2014, pag. 34.

[62] Nel valutare l'impatto sugli interessi, sui diritti e sulle libertà fondamentali dell'interessato, nel contesto del *targeting* rivolto agli utenti di social media, le seguenti considerazioni sono particolarmente rilevanti: i) le finalità del *targeting*; ii) il livello di dettaglio dei criteri di *targeting* utilizzati (ad esempio una coorte descritta in maniera ampia come "persone interessate alla letteratura inglese" o criteri più dettagliati per consentire la segmentazione e il *targeting* a un livello più granulare); iii) il tipo (e la combinazione) di criteri di *targeting* utilizzati (ossia se il *targeting* si concentra soltanto su uno specifico aspetto dell'interessato o se ha una natura più esaustiva); e iv) la natura (sensibilità), il volume e la fonte dei dati utilizzati per sviluppare i criteri di *targeting*. Cfr. Gruppo di lavoro Articolo 29, Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, WP 217, 9 aprile 2014, https://ec.europa.eu/justice/article 29/documentation/opinion-recommendation/files/2014/wp217_it.pdf.

[63] Gruppo di lavoro Articolo 29, Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, WP 251, rev. 01, pag. 16; cfr. anche Gruppo di lavoro Articolo 29, Parere 6/2014 sul concetto di interesse legittimo, pag. 38 e 56: "[n]el complesso, esiste uno squilibrio tra l'interesse legittimo della società e la protezione dei diritti fondamentali degli utenti e l'articolo 7, lettera f), non deve essere invocato come fondamento giuridico per il trattamento. Sarebbe più opportuno utilizzare l'articolo 7, lettera a), come fondamento giuridico purché siano soddisfatte le condizioni per un consenso valido".

[64] Cfr. Gruppo di lavoro Articolo 29, Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, WP 259, rev. 01.

[65] Cfr. Gruppo di lavoro Articolo 29, Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, WP 259, rev. 01, pag. 4.

[66] Cfr. EDPB, Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della

fornitura di servizi online agli interessati, versione 2.0, 8 ottobre 2019, disponibile all'indirizzo:
https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_it.pdf.

[67] Nelle situazioni in cui gli indirizzi di posta elettronica sono utilizzati per inviare comunicazioni di marketing diretto agli utenti, i titolari del trattamento devono altresì tenere conto delle disposizioni di cui all'articolo 13 della direttiva e-privacy.

[68] La determinazione delle finalità e dei mezzi del trattamento del *targeter* e del fornitore di social media è simile (anche se non identica) all'esempio 1. Caricando l'elenco degli indirizzi di posta elettronica e impostando i criteri di *targeting* aggiuntivi, il *targeter* definisce i criteri in base ai quali avviene il *targeting* e designa le categorie di persone i cui dati personali devono essere utilizzati. Il fornitore di social media determina analogamente quali dati personali saranno trattati, definendo quali categorie di dati saranno trattati, quali criteri di *targeting* saranno offerti e chi avrà accesso a (quali tipi di) dati personali trattati nel contesto di una particolare campagna di *targeting*. La finalità condivisa alla base di tali trattamenti somiglia alla finalità individuata nell'esempio 1, ossia la presentazione di pubblicità specifica a un insieme di persone fisiche (nel caso di specie: gli utenti di social media) che costituiscono la platea di destinatari.

[69] I pixel di tracciamento sono costituiti da piccoli frammenti di codice che sono integrati nel sito web del *targeter*. Quando una persona accede al sito web del *targeter* nel suo browser, quest'ultimo invia automaticamente una richiesta al server del fornitore di social media per ottenere il pixel di tracciamento. Una volta scaricato il pixel di tracciamento, il fornitore di social media è in genere in grado di monitorare la sessione dell'utente (ossia il comportamento della persona sul sito web in questione). I dati osservati possono essere utilizzati ad esempio per aggiungere un utente di social media a un particolare pubblico destinatario.

[70] Un fornitore di social media può altresì essere in grado di determinare la posizione dei propri utenti sulla base di altri dati, tra i quali l'indirizzo IP e le informazioni WiFi ottenute dai dispositivi mobili o i dati derivati dall'utente (ad esempio se inseriscono informazioni sulla loro posizione in un post sulla piattaforma).

[71] Corte di giustizia dell'Unione europea, sentenza nella causa Planet49 Gmbh, C 673/17, ECLI:EU:C:2019:801, punto 73.

[72] Cfr. parere 5/2019 sull'interazione tra la direttiva e-privacy e il regolamento generale sulla protezione dei dati, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati. Cfr. anche Corte di giustizia dell'Unione europea, sentenza nella causa Fashion ID, C-40/17, punti da 89 a 91.

[73] *Ibidem*, punto 74.

[74] EDPB, Linee guida 05/2020 sul consenso ai sensi del regolamento 2016/679, versione 1.1, pag. 6.

[75] Corte di giustizia dell'Unione europea, sentenza nella causa Planet 49 GmbH, C-637/17, punto 57.

[76] EDPB, Linee guida 05/2020 sul consenso ai sensi del regolamento 2016/679, versione 1.1, pag. 21.

[77] EDPB, Linee guida 05/2020 sul consenso ai sensi del regolamento 2016/679, versione 1.1, pag. 17, punto 65.

[78] Sentenza della Corte di giustizia dell'Unione europea del 29 luglio 2019 nella causa Fashion ID, C-40/17, ECLI:EU:C:2019:629, punti 100 e 101.

[79] Ciò è tanto più vero nella misura in cui per la maggior parte degli strumenti di *targeting*, è il social media che esegue le operazioni di lettura/scrittura sul terminale dell'utente, dato che raccoglie i dati personali per finalità di pubblicità mirata. Di conseguenza al fornitore di social media spetta la responsabilità di assicurare che sia stato ottenuto un consenso valido.

[80] EDPB, Parere 5/2019 sull'interazione tra la direttiva e-privacy e il regolamento generale sulla protezione dei dati, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati, punto 41.

[81] Gruppo di lavoro Articolo 29, Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, WP 251, rev. 01, pag. 16; cfr. anche Gruppo di lavoro Articolo 29, Parere 6/2014 sul concetto di interesse legittimo, pag. 38 e 56: "[n]el complesso, esiste uno squilibrio tra l'interesse legittimo della società e la protezione dei diritti fondamentali degli utenti e l'articolo 7, lettera f), non deve essere invocato come fondamento giuridico per il trattamento. Sarebbe più opportuno utilizzare l'articolo 7, lettera a), come fondamento giuridico purché siano soddisfatte le condizioni per un consenso valido".

[82] EDPB, Parere 5/2019 sull'interazione tra la direttiva e-privacy e il regolamento generale sulla protezione dei dati, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati, punto 41.

[83] EDPB, Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, versione 2.0, 8 ottobre 2019, punto 1.

[84] Cfr. anche Gruppo di lavoro Articolo 29, Linee guida sul diritto alla portabilità dei dati, WP 242 rev. 01, 5 aprile 2017, pag. 11.

[85] Per quanto riguarda le pagine dei social media, le condizioni di contitolarità possono essere soddisfatte anche in relazione a informazioni statistiche erogate dal fornitore di social media all'amministratore della pagina: cfr. Sentenza della Corte di giustizia dell'Unione europea nella causa Wirtschaftsakademie, C-210/16.

[86] L'EDPB osserva che la profilazione può essere avvenuta anche in esempi precedenti.

[87] Gruppo di lavoro, Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, WP 251 rev. 01, pag. 7.

[88] Gruppo di lavoro, Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, WP 251 rev. 01, pagg. 24-25.

[89] Cfr. anche Gruppo di lavoro Articolo 29, Linee guida sulla trasparenza ai sensi del regolamento 2016/679, WP 260 rev. 01, 11 aprile 2018, https://ec.europa.eu/newsroom/article29/items/622227/en.

[90] Riferimento a EDPB, Linee guida sulla trasparenza ai sensi del regolamento 2016/679.

[91] Gruppo di lavoro Articolo 29, Linee guida sul consenso ai sensi del regolamento 2016/679, WP 259 rev. 01, punti 24 e 35.

[92] Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento", WP 169, pag. 29.

[93] Corte di giustizia dell'Unione europea, sentenza Fashion ID, punti 102 e 105.

[94] Come chiarito nelle linee guida 7/2020 dell'EDPB sui concetti di responsabile del trattamento e di titolare del trattamento nel GDPR, ciascun titolare del trattamento è soggetto all'obbligo di garantire che i dati non siano ulteriormente trattati in maniera incompatibile con le finalità per le quali sono stati originariamente raccolti dal titolare del trattamento che condivide i dati. Sarebbe buona prassi che il titolare del trattamento che intende trattare i dati personali per ulteriori finalità fornisca elementi sufficienti all'altro titolare del trattamento che gli trasmette i dati personali in modo da accertare la sussistenza effettiva di una base giuridica, che sarebbe probabilmente il consenso, e l'adeguata informazione degli interessati, in quanto ciò consentirebbe al *targeter* di garantire la liceità del trasferimento di dati al fornitore di social media.

[95] L'articolo 15, paragrafi 1 e 2, GDPR specifica le informazioni da fornire all'interessato che chiede l'accesso ai suoi dati. L'articolo 15, paragrafi 3 e 4, GDPR disciplina il diritto di ottenerne una copia.

[96] Cfr. EDPB, Linee guida sulla trasparenza ai sensi del regolamento 2016/679, pag. 37.

[97] Per ulteriori dettagli sulle informazioni ai sensi dell'articolo 15 GDPR nel contesto della profilazione, cfr. Gruppo di lavoro, WP 251 rev. 01, pag. 17 ("*L'articolo 15 conferisce all'interessato il diritto di ottenere informazioni dettagliate sui dati personali utilizzati per la profilazione, ivi comprese le categorie di dati impiegati per creare un profilo. Oltre alle informazioni generali sul trattamento, ai sensi dell'articolo 15, paragrafo 3, il titolare del trattamento deve rendere disponibili i dati utilizzati come input per creare il profilo, e consentire l'accesso alle informazioni sul profilo e ai dettagli dei segmenti nei quali l'interessato è stato inserito*"). È importante che tali informazioni siano adattate alla situazione specifica dell'interessato, integrando qualsiasi informazione già fornita ai sensi degli articoli 1 e 14.

[98] Cfr. EDPB, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento 2016/679, WP 248 rev. 0.

[99] L'EDPB ribadisce che una valutazione d'impatto sulla protezione dei dati non è richiesta quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili al trattamento per il quale tale valutazione è stata effettuata. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo; cfr. Gruppo di lavoro Articolo 29, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, WP 248 rev. 01, pag. 12.

[100] *Ibidem*, pag. 8

[101] Cfr. analisi di cui al capitolo 5.2.1.

[102] Gruppo di lavoro Articolo 29, Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, WP 251 rev. 01, pag. 16.

[103] Nell'esempio 14 non esiste una contitolarità tra il fornitore di social media e IlTuoLavoroPerfetto al momento della raccolta dei dati personali, dato che non determinano congiuntamente le finalità della raccolta e del trattamento successivo o ulteriore dei dati personali per le finalità di IlTuoLavoroPerfetto in tale fase del trattamento. L'EDPB ricorda che l'analisi dei ruoli e delle responsabilità deve essere effettuata caso per caso e che la conclusione su questo esempio specifico non pregiudica qualsiasi altro esercizio che può essere svolto dall'EDPB sulle API. La situazione sarebbe naturalmente diversa se il fornitore di social media, oltre a mettere a disposizione i dati personali, partecipasse anche alla determinazione della finalità perseguita da IlTuoLavoroPerfetto. In ogni caso la contitolarità continua ad esistere tra il *targeter* e il fornitore di social media per quanto riguarda l'uso del *targeting* basato su elenchi.

[104] Il Gruppo di lavoro ha chiarito nel suo parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia (WP 258, 29/11/2017, pag. 11) che l'espressione "resi manifestamente pubblici dall'interessato" deve essere interpretata nel senso che essa implica che l'interessato sia consapevole che i rispettivi dati saranno resi disponibili pubblicamente, ossia per tutti, autorità comprese. Quindi, "[i]n caso di dubbio, dovrebbe essere applicata un'interpretazione restrittiva".

[105] Sentenza della Corte di giustizia dell'Unione europea del 5 giugno 2018, Wirtschaftsakademie, C-210/16, punto 43.

[106] Cfr. anche Corte di giustizia dell'Unione europea, sentenza Google Spain nella causa C-131/12, ECLI:EU:C:2014:317 ("responsabilità, competenze e possibilità").

[107] L'EDPB ritiene che in molti casi una valutazione basata sui criteri di cui sopra (ad esempio i dati utilizzati per stabilire i criteri di *targeting*, l'abbinamento dell'interessato, la raccolta del consenso) porterà probabilmente a constatare che è il fornitore di social media il soggetto ad avere una maggiore influenza concreta sul trattamento e pertanto un grado di responsabilità più elevato, a seconda del meccanismo specifico di *targeting* utilizzato.

[108] Inoltre, dato che MiglioriBorse.com ha integrato il pixel di tracciamento del social media nel proprio sito web, è altresì responsabile del rispetto delle prescrizioni di cui alla direttiva e-privacy per quanto concerne questo strumento, il quale, dato che il pixel facilita anche il trattamento di dati personali, è anch'esso importante per determinare il livello di responsabilità.

Linee guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali Versione 2.0

Adottate il 14 dicembre 2021

Cronologia delle versioni

Versione 2.0	14 dicembre 2021	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	14 gennaio 2021	Adozione delle linee guida per consultazione pubblica

Indice

Linee guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali

1 Introduzione

2 Ransomware
- 2.1 Caso n. 01: Ransomware in presenza di backup adeguato e senza esfiltrazione
  - 2.1.1 Caso n. 01 — Misure in essere e valutazione del rischio
  - 2.1.2 Caso n. 01 — Misure di mitigazione e obblighi
- 2.2 Caso n. 02: Ransomware senza un adeguato backup
  - 2.2.1 Caso n. 02 — Misure in essere e valutazione del rischio
  - 2.2.2 Caso n. 02 — Misure di mitigazione e obblighi
- 2.3 Caso n. 03: Attacco ransomware nei confronti di un ospedale con backup e senza esfiltrazione
  - 2.3.1 Caso n. 03 — Misure in essere e valutazione del rischio
  - 2.3.2 Caso n. 03 — Misure di mitigazione e obblighi
- 2.4 Caso n. 04: Attacco ransomware senza backup e con esfiltrazione
  - 2.4.1 Caso n. 04 — Misure in essere e valutazione del rischio
  - 2.4.2 Caso n. 04 — Misure di mitigazione e obblighi
- 2.5 Misure organizzative e tecniche per prevenire/mitigare gli effetti degli attacchi di ransomware

3 Attacchi di esfiltrazione dei dati
- 3.1 Caso n. 05: Esfiltrazione dei dati delle domande di impiego da un sito web
  - 3.1.1 Caso n. 05 — Misure in essere e valutazione del rischio
  - 3.1.2 Caso n. 05 — Misure di mitigazione e obblighi
- 3.2 Caso n. 06: Esfiltrazione da un sito web di password sottoposte ad hashing
  - 3.2.1 Caso n. 06 — Misure in essere e valutazione del rischio
  - 3.2.2 Caso n. 06 — Misure di mitigazione e obblighi
- 3.3 Caso n. 07: Attacco del tipo credential stuffing su un sito web bancario
  - 3.3.1 Caso n. 07 — Misure in essere e valutazione del rischio
  - 3.3.2 Caso n. 07 — Misure di mitigazione e obblighi
- 3.4 Misure organizzative e tecniche per prevenire/mitigare gli effetti degli attacchi di hacker

4 Fonti di rischio interne legate al fattore umano
4.1 Caso n. 08: Esfiltrazione di dati aziendali da parte di un dipendente
4.1.1 Caso n. 08 — Misure in essere e valutazione del rischio
4.1.2 Caso n. 08 — Misure di mitigazione e obblighi
4.2 Caso n. 09: Trasmissione accidentale di dati a un terzo fidato
4.2.1 Caso n. 09 — Misure in essere e valutazione del rischio
4.2.2 Caso n. 09 — Misure di mitigazione e obblighi
4.3 Misure organizzative e tecniche per prevenire/attenuare l'impatto delle fonti interne di rischio legate al fattore umano

5 Smarrimento o furto di dispositivi o di documenti cartacei
5.1 Caso n. 10: Furto di supporti sui quali sono memorizzati dati personali cifrati
5.1.1 Caso n. 10 — Misure in essere e valutazione del rischio
5.1.2 Caso n. 10 — Misure di mitigazione e obblighi
5.2 Caso n. 11: Furto di supporti sui quali sono memorizzati dati personali non cifrati
5.2.1 Caso n. 11 — Misure in essere e valutazione del rischio
5.2.2 Caso n. 11 — Misure di mitigazione e obblighi
5.3 Caso n. 12 – Furto di fascicoli cartacei contenenti dati sensibili
5.3.1 Caso n. 12 — Misure in essere e valutazione del rischio
5.3.2 Caso n. 12 — Misure di mitigazione e obblighi
5.4 Misure organizzative e tecniche per prevenire/attenuare le conseguenze della perdita o del furto di dispositivi

6 Errato invio di corrispondenza
6.1 Caso n. 13: Errore nella corrispondenza postale
6.1.1 Caso n. 13 — Misure in essere e valutazione del rischio
6.1.2 Caso n. 13 — Misure di mitigazione e obblighi
6.2 Caso n. 14: Dati personali altamente riservati inviati erroneamente per posta elettronica
6.2.1 Caso n. 14 — Misure in essere e valutazione del rischio
6.2.2 Caso n. 14 — Misure di mitigazione e obblighi
6.3 Caso n. 15: Dati personali inviati per errore tramite posta elettronica
6.3.1 Caso n. 15 — Misure in essere e valutazione del rischio
6.3.2 Caso n. 15 — Misure di mitigazione e obblighi
6.4 Caso n. 16: Errore nell'invio di corrispondenza postale
6.4.1 Caso n. 16 — Misure in essere e valutazione del rischio
6.4.2 Caso n. 16 — Misure di mitigazione e obblighi
6.5 Misure organizzative e tecniche per prevenire/attenuare gli effetti di un'errata postalizzazione

7 ALTRI CASI — INGEGNERIA SOCIALE (Social Engineering)
7.1 Caso n. 17: Furto d'identità
7.1.1 Caso n. 17 — Valutazione del rischio, misure di mitigazione e obblighi
7.2 Caso n. 18: Esfiltrazione di e-mail
7.2.1 Caso n. 18 — Valutazione del rischio, misure di mitigazione e obblighi

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

Visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in appresso "GDPR"),

Visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37 dello stesso, modificati dalla Dichiarazione del 6 luglio 2018[1],

Visti l'articolo 12 e l'articolo 22 del suo regolamento,

Vista la comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo "La protezione dei dati quale pilastro della responsabilizzazione dei cittadini e dell'approccio dell'UE alla transizione digitale — due anni di applicazione del regolamento generale sulla protezione dei dati"[2],

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

1. INTRODUZIONE

1. Il GDPR introduce, in alcuni casi, l'obbligo di notificare una violazione dei dati personali all'autorità nazionale di controllo competente e di comunicare la violazione alle persone i cui dati personali sono stati interessati dalla violazione (articoli 33 e 34).
2. Nell'ottobre 2017 il gruppo di lavoro "Articolo 29" ha già elaborato linee guida generali sulla notifica delle violazioni dei dati, analizzando le sezioni pertinenti del regolamento generale sulla protezione dei dati (Linee guida sulla notifica delle violazioni dei dati personali a norma del regolamento (UE) 2016/679, WP 250) (di seguito "Linee guida WP250"[3]). Tuttavia, a causa della loro natura e della tempistica prevista, tali linee guida non hanno affrontato tutte le questioni pratiche in modo sufficientemente dettagliato. Pertanto, è emersa la necessità di una guida pratica e basata su casi concreti, che utilizzi le esperienze acquisite dalle autorità di controllo da quando GDPR è divenuto pienamente applicabile.
3. Il presente documento è inteso a integrare gli orientamenti WP 250 e rispecchia le esperienze comuni delle autorità di controllo dello Spazio Economico Europeo (SEE) successivamente alla piena applicabilità del regolamento generale sulla protezione dei dati. Il suo obiettivo è aiutare i titolari del trattamento a decidere come gestire le violazioni dei dati e quali fattori prendere in considerazione durante la valutazione del rischio.
4. Qualsiasi tentativo di porre rimedio a una violazione presuppone che il titolare e il responsabile del trattamento siano in grado di riconoscerla. L'articolo 4, paragrafo 12, del regolamento generale sulla protezione dei dati definisce una "violazione dei dati personali" come "una violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o altrimenti trattati".
5. Nel suo parere 03/2014 sulla notifica delle violazioni[4] e nelle Linee guida WP 250, il WP29 ha spiegato che le violazioni possono essere classificate in base ai seguenti tre noti principi di sicurezza delle informazioni:

- "Violazione della riservatezza" — in caso di divulgazione non autorizzata o accidentale di dati personali o di accesso non autorizzato o accidentale agli stessi.
- "Violazione dell'integrità" — in caso di modifica non autorizzata o accidentale di dati personali.
- "Violazione della disponibilità" — in caso di perdita accidentale o non autorizzata dell'accesso ai dati personali o di loro distruzione accidentale o non autorizzata.[5]

6. Una violazione può avere potenzialmente numerosi effetti negativi significativi sulle persone fisiche, che possono causare danni fisici, materiali o immateriali. Il GDPR spiega che ciò può includere la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie,

la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo per le persone fisiche interessate. Uno degli obblighi più importanti del titolare del trattamento è valutare tali rischi per i diritti e le libertà degli interessati e attuare misure tecniche e organizzative adeguate per affrontarli.

7. Di conseguenza, il GDPR impone al titolare del trattamento di:

- documentare le violazioni dei dati personali, comprese le circostanze della violazione dei dati personali, le sue conseguenze e le azioni correttive adottate;[6]
- notificare la violazione dei dati personali all'autorità di controllo, a meno che sia improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche;[7]
- comunicare la violazione dei dati personali all'interessato quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.[8]

8. Le violazioni dei dati sono di per sé problematiche, ma possono anche essere sintomi di un regime di sicurezza dei dati vulnerabile e forse obsoleto, oppure segnalare carenze del sistema da affrontare. In linea generale, è sempre meglio prevenire le violazioni dei dati preparandosi in anticipo, dal momento che diverse conseguenze sono per loro natura irreversibili. Prima che un titolare del trattamento possa valutare appieno il rischio derivante da una violazione causata da una qualche forma di attacco, occorre individuare la causa alla radice del problema, al fine di stabilire se le vulnerabilità che hanno determinato l'incidente siano ancora presenti e siano pertanto ancora sfruttabili. In molti casi il titolare del trattamento è in grado di individuare che l'incidente può comportare un rischio e deve pertanto essere notificato. In altri casi non si dovrà rinviare la notifica fino a quando il rischio e l'impatto della violazione non siano stati pienamente valutati, poiché la valutazione completa del rischio può avvenire parallelamente alla notifica e le informazioni così ottenute possono essere fornite all'autorità di controllo in fasi successive senza ulteriore e ingiustificato ritardo.[9]

9. La violazione dovrebbe essere notificata quando il titolare del trattamento ritiene che possa comportare un rischio per i diritti e le libertà dell'interessato. I titolari dovrebbero effettuare tale valutazione nel momento in cui vengono a conoscenza della violazione. Un titolare non dovrebbe attendere gli esiti di un'analisi forense dettagliata e l'applicazione di azioni di mitigazione del rischio (precoci) prima di valutare se la violazione dei dati possa comportare un rischio e debba pertanto essere notificata.

10. Se un titolare del trattamento valuta autonomamente che un rischio sia improbabile, ma tale rischio di fatto si concretizza, l'autorità di controllo competente può avvalersi dei suoi poteri correttivi e può decidere di comminare sanzioni.

11. Ogni titolare e responsabile del trattamento dovrebbe disporre di piani e procedure per la gestione di eventuali violazioni dei dati. Si dovrebbero prevedere linee gerarchiche chiare e specifiche figure responsabili di determinati aspetti del processo di recupero.

12. Anche la formazione e la sensibilizzazione in materia di protezione dei dati per il personale del titolare e del responsabile del trattamento sono essenziali, concentrandosi sulla gestione delle violazioni dei dati personali (identificazione di un incidente di violazione dei dati personali e ulteriori azioni da intraprendere, ecc.). Tale formazione dovrebbe essere ripetuta periodicamente, a seconda del tipo di trattamento e delle dimensioni della struttura del titolare, esaminando le più recenti tendenze e segnalazioni derivanti da attacchi informatici o altri incidenti di sicurezza.
13. Il principio di responsabilizzazione e il concetto di protezione dei dati fin dalla progettazione potrebbero contemplare un'analisi intesa a confluire in una sorta di "Manuale per la gestione delle violazioni dei dati" messo a punto dal titolare e dal responsabile del trattamento, in cui definire gli elementi fattuali in rapporto a ogni sfaccettatura del trattamento in ciascuna delle fasi principali dell'operazione. Tale manuale, ove redatto preventivamente, fornirebbe una fonte di informazioni molto più rapida per consentire ai titolari e ai responsabili del trattamento di mitigare i rischi e di adempiere ai rispettivi obblighi senza indebito ritardo. Così facendo, in caso di violazione dei dati personali, il personale saprà cosa fare e l'incidente potrà essere gestito più rapidamente di quanto avverrebbe in assenza di misure di mitigazione o dei predetti piani.
14. Sebbene i casi presentati di seguito siano fittizi, essi si basano su casi tipici tratti dall'esperienza collettiva delle autorità di controllo in materia di notifiche di violazioni dei dati. Le analisi proposte si riferiscono esplicitamente ai casi in esame, ma con l'obiettivo di fornire assistenza ai titolari del trattamento per la valutazione delle violazioni dei dati che li riguardino. Qualsiasi modifica delle circostanze riferite alle fattispecie descritte di seguito può comportare livelli di rischio diversi o più significativi, e quindi rendere necessarie misure diverse o supplementari. In queste linee guida, i casi sono presentati in base a determinate categorie di violazioni (ad esempio "attacchi ransomware"). Alcune misure di mitigazione sono necessarie in tutte le fattispecie appartenenti a una determinata categoria di violazioni. Tali misure non sono necessariamente ripetute in ciascuna analisi riferita a un caso appartenente alla stessa categoria di violazioni. Per i casi appartenenti alla stessa categoria sono indicate solo le differenze. Pertanto, il lettore dovrebbe tenere conto dell'intera casistica riferita alla pertinente categoria di violazione al fine di individuare e distinguere tutte le misure corrette da adottare.
15. La documentazione interna di una violazione è un obbligo indipendente dai rischi connessi alla violazione stessa e deve essere predisposta in ogni singolo caso. I casi presentati di seguito cercano di chiarire se notificare o meno la violazione all'autorità di controllo e comunicarla agli interessati coinvolti.

2. RANSOMWARE

16. Una causa frequente di notifica di violazione dei dati è un attacco ransomware subito dal titolare del trattamento. In questi casi un codice malevolo cifra

i dati personali e successivamente l'autore dell'attacco chiede al titolare del trattamento un riscatto in cambio della chiave di decifratura. Questo tipo di attacco può di norma essere classificato come una violazione della disponibilità, ma spesso potrebbe comportare anche una violazione della riservatezza.

2.1 CASO N. 01: RANSOMWARE IN PRESENZA DI BACKUP ADEGUATO E SENZA ESFILTRAZIONE

I sistemi informatici di una piccola impresa manifatturiera sono stati esposti a un attacco ransomware e i dati memorizzati in tali sistemi sono stati cifrati. Il titolare ha utilizzato la cifratura dei dati memorizzati (at rest), per cui tutti i dati ai quali ha avuto accesso il ransomware erano conservati in forma cifrata utilizzando un algoritmo di cifratura conforme allo stato dell'arte. La chiave di decifratura non è stata compromessa nell'attacco, ossia l'autore dell'attacco non ha potuto accedervi né utilizzarla indirettamente. Di conseguenza, l'autore dell'attacco ha avuto accesso solo a dati personali cifrati. In particolare, né il sistema di posta elettronica della società né i sistemi clienti utilizzati per accedervi sarebbero stati interessati. L'impresa si avvale delle competenze di una società esterna di cybersecurity per indagare sull'incidente. Sono disponibili le registrazioni (log) di tutti i flussi dati in uscita dall'impresa (compresa la posta elettronica in uscita). Dopo aver analizzato i log e i dati raccolti dai sistemi di rilevazione utilizzati dall'impresa, un'indagine interna supportata dalla società esterna di cybersecurity ha stabilito con *certezza* che l'autore del reato si è limitato a cifrare i dati, senza esfiltrarli. I log non mostrano alcun flusso di dati verso l'esterno nell'arco di tempo dell'attacco. I dati personali interessati dalla violazione riguardano i clienti e i dipendenti dell'impresa, per un totale di poche decine di persone. Un backup era prontamente disponibile e i dati sono stati ripristinati poche ore dopo l'attacco. La violazione non ha avuto alcuna conseguenza sull'operatività del titolare del trattamento. Non vi sono stati ritardi nei pagamenti dei dipendenti o nella gestione delle richieste dei clienti.

17. In questo caso, rispetto alla definizione di "violazione dei dati personali" si sono concretizzati i seguenti elementi: una violazione della sicurezza ha comportato una modifica illecita e l'accesso non autorizzato ai dati personali conservati.

2.1.1 CASO N. 01 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

18. Come per tutti i rischi posti da attori esterni, la probabilità che un attacco ransomware abbia successo può essere drasticamente ridotta rafforzando la sicurezza dei dati mediante controllo del contesto. La maggior parte di queste violazioni può essere evitata garantendo l'adozione di adeguate misure di sicurezza organizzative, fisiche e tecnologiche. Esempi di tali misure sono la corretta gestione delle patch e l'uso di un adeguato sistema di rilevamento di

malware. Disporre di un backup adeguato e separato contribuirà ad attenuare le conseguenze di un eventuale attacco riuscito. Inoltre, un programma di istruzione, formazione e sensibilizzazione dei dipendenti in materia di sicurezza (SETA) contribuirà a prevenire e riconoscere questo tipo di attacco. (Un elenco di misure consigliate è riportato nella sezione 2.5.) Tra tali misure, una delle più importanti è una corretta gestione delle patch che assicuri che i sistemi siano aggiornati e che tutte le vulnerabilità note dei sistemi installati siano state corrette poiché la maggior parte degli attacchi ransomware sfrutta proprio vulnerabilità ben note.

19. Nel valutare i rischi, il titolare del trattamento dovrebbe indagare sulla violazione e individuare il tipo di codice malevolo per comprendere le possibili conseguenze dell'attacco. Tra i rischi da considerare figura il rischio che i dati siano stati esfiltrati senza lasciare traccia nei log dei sistemi.

20. In questo esempio, l'attaccante ha avuto accesso ai dati personali ed è stata compromessa la riservatezza del testo cifrato contenente dati personali in forma cifrata. Tuttavia, i dati che potrebbero essere stati esfiltrati non possono essere letti o utilizzati dall'autore dell'attacco, almeno per il momento. La tecnica di cifratura utilizzata dal titolare è conforme allo stato dell'arte. La chiave di decifratura non è stata compromessa e presumibilmente non può essere determinata con altri mezzi. Di conseguenza, i rischi in termini di riservatezza per i diritti e le libertà delle persone fisiche sono ridotti al minimo, salvi i progressi delle tecniche crittografiche che in futuro potrebbero rendere i dati cifrati intelligibili.

21. Il titolare del trattamento dovrebbe considerare il rischio per le persone fisiche dovuto alla violazione[10]. In questo caso, sembra che i rischi per i diritti e le libertà degli interessati derivino dalla mancanza di disponibilità dei dati personali e che la riservatezza dei dati personali non sia compromessa[11]. In questo esempio, gli effetti negativi della violazione sono stati attenuati in tempi contenuti dopo il verificarsi della violazione stessa. Disporre di un adeguato regime di backup[12] riduce gli effetti negativi della violazione e in questo caso il titolare del trattamento è stato in grado di avvalersene in modo efficace.

22. Per quanto riguarda la gravità delle conseguenze per gli interessati, è stato possibile individuare solo conseguenze minori, poiché i dati sono stati ripristinati in poche ore e la violazione non ha avuto conseguenze sull'operatività del titolare del trattamento né effetti significativi sugli interessati (ad esempio pagamenti ai dipendenti o gestione delle richieste dei clienti).

2.1.2 CASO N. 01 — MISURE DI MITIGAZIONE E OBBLIGHI

23. In assenza di un backup, il titolare del trattamento può adottare poche misure per porre rimedio alla perdita di dati personali e i dati devono essere nuovamente raccolti. In questo caso particolare, tuttavia, gli effetti dell'attacco potrebbero essere contenuti efficacemente "ripulendo" tutti i sistemi compromessi dal codice malevolo, correggendo le vulnerabilità e ripristinando i dati interessati entro breve tempo dall'attacco. In assenza di backup, i dati

sarebbero andati persi e la gravità può aumentare di pari passo con i rischi o gli impatti per le persone.

24. La tempestività di un ripristino efficace dei dati utilizzando un backup prontamente disponibile è una variabile fondamentale nell'analisi della violazione. La definizione di una tempistica adeguata per il ripristino di dati compromessi dipende dalle circostanze specifiche della violazione. Il regolamento generale sulla protezione dei dati stabilisce che una violazione dei dati personali deve essere notificata senza ingiustificato ritardo e, ove possibile, entro 72 ore. Si potrebbe pertanto stabilire che in nessun caso è consigliabile superare il termine di 72 ore, ma quando si tratta di casi caratterizzati da un rischio elevato, anche il rispetto di tale termine può risultare insoddisfacente.
25. In questo caso, grazie a procedure dettagliate per la valutazione d'impatto e la risposta agli incidenti, il titolare del trattamento ha stabilito che era improbabile che la violazione comportasse un rischio per i diritti e le libertà delle persone fisiche; pertanto non è necessaria alcuna comunicazione agli interessati, né la violazione richiede una notifica all'autorità di controllo. Tuttavia, come tutte le violazioni dei dati, è necessario conservarne la documentazione conformemente all'articolo 33, paragrafo 5. La struttura del titolare potrebbe anche necessitare di (o essere successivamente tenuta a effettuare, su disposizione dell'autorità di controllo) aggiornamenti e correzioni delle misure e procedure organizzative e tecniche messe in atto per la gestione della sicurezza dei dati personali e la mitigazione dei rischi. Nell'ambito di tale aggiornamento e revisione, si dovrebbe indagare approfonditamente sulla violazione individuandone le cause e definendo i metodi utilizzati dall'autore dell'attacco al fine di prevenire eventi analoghi in futuro.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	√	X

2.2 CASO N. 02: RANSOMWARE SENZA UN ADEGUATO BACKUP

Uno dei computer utilizzati da un'azienda agricola è stato esposto a un attacco ransomware e i dati sono stati cifrati dall'attaccante. L'impresa si avvale delle competenze di una società esterna di cybersecurity per monitorare la propria rete. Sono disponibili log che tracciano tutti i flussi di dati in uscita dall'impresa (comprese le e-mail in uscita). Dopo aver analizzato i log e i dati raccolti dagli altri sistemi di rilevamento, l'indagine interna condotta con l'ausilio dell'impresa di cybersecurity ha stabilito che l'autore dell'attacco ha soltanto cifrato i dati, senza esfiltrarli. I log non mostrano alcun flusso di dati verso l'esterno nell'arco di tempo dell'attacco.

I dati personali interessati dalla violazione riguardano i dipendenti e i clienti dell'impresa, per un totale di poche decine di persone. Non sono state interessate categorie particolari di dati. Non era disponibile alcun backup in formato elettronico. La maggior parte dei dati è stata ripristinata da backup cartacei. Il ripristino dei dati ha richiesto 5 giorni lavorativi e ha comportato lievi ritardi nella consegna degli ordini ai clienti.

2.2.1 CASO N. 02 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

26. Il titolare del trattamento avrebbe dovuto adottare le stesse misure di cui alla parte 2.1 e alla sezione 2.9. La principale differenza rispetto al caso precedente è la mancanza di un backup in formato elettronico e la mancanza di cifratura dei dati memorizzati (at rest). Ciò comporta differenze critiche nelle fasi successive.
27. Nel valutare i rischi, il titolare del trattamento dovrebbe indagare sul metodo di infiltrazione e individuare la tipologia di codice malevolo per comprendere le possibili conseguenze dell'attacco. In questo esempio il ransomware cifrava i dati personali senza esfiltrarli. Di conseguenza, i rischi per i diritti e le libertà degli interessati sembrano derivare dalla mancanza di disponibilità dei dati personali e la riservatezza dei dati personali non risulterebbe compromessa. Per determinare il rischio è essenziale un esame approfondito dei log dei firewall e delle relative implicazioni. Su richiesta, il titolare del trattamento dovrebbe presentare le risultanze documentate di tali indagini.
28. Il titolare del trattamento deve tenere presente che, se l'attacco è più sofisticato, il malware è in grado di modificare i file di log e rimuovere le tracce. Pertanto, poiché i log non sono trasmessi o replicati a un server centrale, anche dopo un'indagine approfondita che ha accertato che i dati personali non sono stati esfiltrati dall'attaccante, il titolare del trattamento non può affermare che l'assenza di log dimostri l'assenza di esfiltrazione; ne consegue l'impossibilità di escludere in via assoluta la probabilità di una violazione della riservatezza.
29. Il titolare del trattamento dovrebbe valutare i rischi di questa violazione[13] se l'attaccante ha avuto accesso ai dati. Nel corso della valutazione del rischio, il titolare dovrebbe tenere conto anche della natura, della sensibilità, del volume e del contesto dei dati personali interessati dalla violazione. In questo caso non sono coinvolte categorie particolari di dati personali e la quantità di dati violati e il numero di interessati colpiti sono ridotti.
30. La raccolta di informazioni esatte sull'accesso non autorizzato è fondamentale per determinare il livello di rischio e prevenire un nuovo attacco o la prosecuzione di un attacco in corso. Se i dati fossero stati copiati dalla banca dati, ciò sarebbe stato ovviamente un fattore di incremento del rischio. In caso di incertezza circa le specificità dell'accesso illegittimo, si dovrebbe prendere in considerazione lo scenario peggiore e il rischio dovrebbe essere valutato in termini conseguenti.
31. L'assenza di un backup può essere considerata un fattore di incremento del

rischio a seconda della gravità delle conseguenze derivanti per gli interessati dall'indisponibilità dei dati.

2.2.2 CASO N. 02 — MISURE DI MITIGAZIONE E OBBLIGHI

32. In assenza di un backup, sono poche le misure che il titolare del trattamento può adottare per porre rimedio alla perdita di dati personali e i dati devono essere nuovamente raccolti, a meno che sia disponibile un'altra fonte (ad esempio, e-mail di conferma degli ordini). Senza un backup, i dati possono andare persi e la gravità dipenderà dall'impatto per le persone.
33. Il ripristino dei dati non dovrebbe rivelarsi eccessivamente problematico[14] se i dati sono ancora disponibili su supporto cartaceo; tuttavia, data la mancanza di un backup in formato elettronico , si ritiene necessaria una notifica all'autorità di controllo, in quanto il ripristino dei dati ha richiesto un certo tempo e potrebbe causare ritardi nella consegna degli ordini ai clienti mentre potrebbe risultare impossibile recuperare una notevole quantità di metadati (ad esempio log, marcatura temporale).
34. La comunicazione agli interessati in merito alla violazione può dipendere anche dal periodo di indisponibilità dei dati personali e dalle difficoltà che ne potrebbero derivare per l'operatività del titolare del trattamento (ad esempio ritardi nel trasferimento dei pagamenti ai dipendenti). Poiché tali ritardi nei pagamenti e nelle consegne possono comportare perdite finanziarie per le persone i cui dati sono stati compromessi, si potrebbe anche sostenere che la violazione comporti un rischio elevato. Inoltre, potrebbe risultare impossibile evitare di informare gli interessati se il loro contributo è necessario per ripristinare i dati cifrati.
35. Questo caso è un esempio di attacco ransomware con rischi per i diritti e le libertà degli interessati, senza che si raggiunga un rischio elevato. La violazione dovrebbe essere documentata conformemente all'articolo 33, paragrafo 5, e notificata all'autorità di controllo a norma dell'articolo 33, paragrafo 1. La struttura del titolare può anche necessitare di (o ricevere disposizioni dall'autorità di controllo per) aggiornare e correggere le misure e procedure organizzative e tecniche di gestione della sicurezza dei dati personali e di mitigazione dei rischi.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	√	X

2.3 CASO N. 03: ATTACCO RANSOMWARE NEI CONFRONTI DI UN OSPEDALE CON BACKUP E SENZA ESFILTRAZIONE

Il sistema informativo di un ospedale/centro sanitario è stato esposto a un attacco ransomware e una parte significativa dei dati è stata cifrata dall'attaccante. L'azienda sanitaria si avvale delle competenze di una società esterna di cybersecurity per monitorare la propria rete. Sono disponibili log che tracciano tutti i flussi di dati in uscita dall'azienda (comprese le e-mail in uscita). Dopo aver analizzato i log e i dati raccolti dagli altri sistemi di rilevamento, l'indagine interna svolta con l'ausilio della società di cybersecurity ha stabilito che l'autore dell'attacco ha soltanto cifrato i dati senza esfiltrarli. I log non mostrano alcun flusso di dati verso l'esterno nell'arco di tempo dell'attacco. I dati personali interessati dalla violazione riguardano i dipendenti e i pazienti, complessivamente varie migliaia di persone. I backup erano disponibili in formato elettronico. La maggior parte dei dati è stata ripristinata, ma questa operazione ha richiesto 2 giorni lavorativi, causando notevoli ritardi nelle cure rese ai pazienti con annullamento o rinvio di interventi chirurgici e un abbassamento del livello di servizio a causa dell'indisponibilità dei sistemi.

2.2.1 CASO N. 03 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

36. Il titolare del trattamento avrebbe dovuto adottare le stesse misure di cui alla parte 2.1 e alla sezione 2.5. La principale differenza rispetto al caso precedente è l'elevata gravità delle conseguenze per un numero sostanziale di interessati[15].

37. La quantità di dati violati e il numero di interessati colpiti dalla violazione sono elevati, in quanto gli ospedali generalmente trattano grandi quantità di dati. L'indisponibilità dei dati ha un forte impatto su una parte sostanziale degli interessati. Esiste inoltre un rischio residuo di elevata gravità per la riservatezza dei dati dei pazienti.

38. La tipologia della violazione, la natura, la sensibilità e il volume dei dati personali interessati dalla violazione sono importanti. Sebbene esistesse un backup per i dati e questi abbiano potuto essere ripristinati in pochi giorni, sussiste un rischio elevato a causa della gravità delle conseguenze per gli interessati derivanti dall'indisponibilità dei dati al momento dell'attacco e nei giorni successivi.

2.3.2 CASO N. 03 — MISURE DI MITIGAZIONE E OBBLIGHI

39. Si ritiene necessaria una notifica all'autorità di controllo, in quanto si tratta di categorie particolari di dati personali e il ripristino dei dati potrebbe richiedere molto tempo, con notevoli ritardi nelle cure dei pazienti. Comunicare la violazione agli interessati è necessario a causa dell'impatto sui pazienti, anche dopo il ripristino dei dati cifrati. Anche se sono stati criptati dati

relativi a tutti i pazienti trattati in ospedale negli ultimi anni, la violazione ha interessato soltanto i dati relativi ai pazienti che dovevano essere sottoposti a terapie in ospedale durante il periodo di indisponibilità del sistema informatico. Il titolare del trattamento dovrebbe comunicare la violazione dei dati direttamente a tali pazienti. L'eccezione di cui all'articolo 34, paragrafo 3, lettera c), può non rendere necessaria la comunicazione diretta agli altri pazienti, alcuni dei quali possono non essere stati ricoverati in ospedale da più di venti anni. In tal caso, si procede invece a una comunicazione pubblica[16] o a una misura analoga, tramite la quale gli interessati sono informati con pari efficacia. In tal caso, l'ospedale dovrebbe rendere pubblico l'attacco ransomware e i suoi effetti.

40. Questo caso serve da esempio di un attacco ransomware con un rischio elevato per i diritti e le libertà degli interessati. La violazione dovrebbe essere documentata conformemente all'articolo 33, paragrafo 5, notificata all'autorità di controllo in conformità dell'articolo 33, paragrafo 1, e comunicata agli interessati in conformità dell'articolo 34, paragrafo 1. L'azienda sanitaria deve inoltre aggiornare e correggere le misure e procedure organizzative e tecniche di gestione della sicurezza dei dati personali e di mitigazione dei rischi.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	√	√

2.4 CASO N. 04: ATTACCO RANSOMWARE SENZA BACKUP E CON ESFILTRAZIONE

Il server di una società di trasporto pubblico è stato esposto a un attacco ransomware e i dati sono stati cifrati dall'autore dell'attacco. Secondo i risultati dell'indagine interna, l'autore dell'attacco non solo ha cifrato i dati, ma li ha anche esfiltrati. La tipologia dei dati violati consiste nei dati personali di clienti e dipendenti e delle diverse migliaia di persone che utilizzano i servizi della società (ad esempio, per l'acquisto di biglietti online). Oltre ai dati identificativi di base, sono coinvolti nella violazione i numeri dei documenti d'identità e dati finanziari come i dati della carta di credito. Era disponibile un backup, ma anch'esso è stato criptato dall'aggressore.

2.4.1 CASO N. 04 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

41. Il titolare del trattamento avrebbe dovuto adottare le stesse misure di cui alla parte 2.1 e alla sezione 2.5. Sebbene disponibile, anche il backup è stato compromesso dall'attacco. Questa circostanza di per sé solleva interrogativi sulla qualità delle misure di sicurezza informatica in essere e dovrebbe es-

sere oggetto di approfondimenti ulteriori durante l'indagine poiché, in un regime di backup ben progettato, devono essere conservati in modo sicuro più backup senza consentire l'accesso dal sistema principale, altrimenti potrebbero essere compromessi nello stesso attacco. Inoltre, gli attacchi ransomware possono rimanere occulti per giorni cifrando lentamente dati utilizzati di rado. Ciò può rendere inutile l'esecuzione di più backup, per cui dovrebbero essere eseguiti anche backup periodici e poi essere isolati. In tal modo si aumenterebbe la probabilità di recupero seppur con una perdita maggiore di dati.

42. La violazione riguarda non solo la disponibilità dei dati, ma anche la riservatezza, in quanto l'autore dell'attacco può aver modificato e/o copiato i dati dal server. Pertanto, il tipo di violazione comporta un rischio elevato[17].

43. La natura, la sensibilità e il volume dei dati personali aumentano ulteriormente i rischi, poiché il numero di persone interessate è elevato, così come la quantità complessiva di dati personali compromessi. Al di là dei dati identificativi di base, sono coinvolti anche documenti di identità e dati finanziari come i dati della carta di credito. Una violazione dei dati relativa a queste categorie di informazioni presenta di per sé un rischio elevato e i dati oggetto di compromissione, se utilizzati congiuntamente, potrebbero servire, tra l'altro, a realizzare furti di identità o frodi.

44. A causa di errori dei controlli logici o organizzativi del server, i backup sono stati compromessi dal ransomware e ciò ha impedito il ripristino dei dati e aumentato il rischio.

45. Questa violazione dei dati presenta un rischio elevato per i diritti e le libertà delle persone, in quanto potrebbe comportare sia un danno materiale (ad esempio una perdita finanziaria dovuta alla compromissione dei dati della carta di credito) sia immateriale (ad esempio furto o usurpazione d'identità in quanto i dati della carta d'identità sono stati compromessi).

2.4.2 CASO N. 04 — MISURE DI MITIGAZIONE E OBBLIGHI

46. La comunicazione agli interessati è essenziale affinché possano adottare le misure necessarie per evitare danni materiali (ad esempio bloccare le loro carte di credito).

47. Oltre a documentare la violazione ai sensi dell'articolo 33, paragrafo 5, anche in questo caso la notifica all'autorità di controllo è obbligatoria (articolo 33, paragrafo 1) e il titolare del trattamento è altresì tenuto a comunicare la violazione agli interessati (articolo 34, paragrafo 1). Quest'ultima comunicazione potrebbe essere effettuata a ogni singolo interessato, ma per le persone in cui i dati di contatto non sono disponibili, il titolare del trattamento dovrebbe dare pubblica comunicazione purché ciò non sia suscettibile di determinare ulteriori conseguenze negative per gli interessati - ad esempio mediante una notifica sul suo sito web. In quest'ultimo caso è necessaria una comunicazione chiara e precisa, ben visibile sulla homepage del titolare del trattamento, con riferimenti esatti alle pertinenti disposizioni del GDPR. La società può inoltre

dover aggiornare e correggere le misure e procedure organizzative e tecniche di gestione della sicurezza dei dati personali e di mitigazione dei rischi.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	√	√

2.5 MISURE ORGANIZZATIVE E TECNICHE PER PREVENIRE/MITIGARE GLI EFFETTI DEGLI ATTACCHI DI RANSOMWARE

48. Il fatto che si sia verificato un attacco ransomware è solitamente la spia dell'esistenza di una o più vulnerabilità del sistema del titolare del trattamento. Ciò vale anche nei casi di attacchi ransomware con cifratura dei dati personali ma senza esfiltrazione. Indipendentemente dall'esito e dalle conseguenze dell'attacco, non si evidenzierà mai a sufficienza quanto sia cruciale una valutazione complessiva del sistema di sicurezza dei dati, con particolare riguardo alla sicurezza informatica. Le debolezze individuate e le lacune di sicurezza devono essere documentate e affrontate senza indugio.

49. Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

- Mantenere aggiornato il firmware, il sistema operativo e il software applicativo sui server, sui client, sui componenti attivi di rete e su ogni altra macchina presente dulla stessa LAN (compresi i dispositivi Wi-Fi). Garantire l'esistenza di adeguate misure di sicurezza informatica, accertarne l'efficacia e mantenerle regolarmente aggiornate quando il trattamento o le circostanze cambiano o evolvono. Ciò comprende la conservazione di log dettagliati dei patch applicati e della rispettiva marcatura temporale.
- Progettazione e organizzazione di sistemi e infrastrutture di trattamento in modo da segmentare o isolare sistemi e reti di dati per evitare la propagazione di software malevolo all'interno dell'organizzazione e verso sistemi esterni.
- Esistenza di una procedura di backup aggiornata, sicura e testata. I mezzi di supporto per il back-up a medio e lungo termine dovrebbero essere tenuti separati dalla conservazione dei dati operativi e fuori dalla portata di soggetti terzi anche in caso di attacco riuscito (per esempio, un backup incrementale giornaliero e un backup settimanale completo).
- Disporre di/procurarsi un software antimalware adeguato, aggiornato, efficace e integrato.

- Disporre di un firewall e sistemi per il rilevamento e la prevenzione delle intrusioni adeguati, aggiornati, efficaci e integrati. Instradare il traffico di rete attraverso il firewall/il sistema rilevamento intrusioni, anche in caso di lavoro agile o in mobilità (ad esempio utilizzando connessioni VPN dotate di meccanismi organizzativi di sicurezza per l'accesso a Internet).
- Formazione dei dipendenti sui metodi di riconoscimento e prevenzione degli attacchi informatici. Il titolare del trattamento dovrebbe fornire gli strumenti per stabilire se le e-mail e i messaggi ottenuti con altri mezzi di comunicazione siano autentici e affidabili. I dipendenti dovrebbero essere formati per riconoscere quando si verifica un attacco del genere, sapere come rimuovere dalla rete l'endpoint ed essere tenuti a segnalarlo immediatamente al responsabile della sicurezza.
- Sottolineare la necessità di individuare il tipo di codice malevolo per comprendere le conseguenze dell'attacco ed essere in grado di individuare le misure giuste per attenuare il rischio. Nel caso in cui un attacco ransomware abbia avuto successo e non sia disponibile alcun back-up, per recuperare i dati possono essere utilizzati strumenti come quelli del progetto "no more ransom" (nomoreransom.org). Tuttavia, nel caso in cui sia disponibile un backup sicuro, è consigliabile ripristinare i dati attraverso il backup.
- Inoltrare o replicare tutti i log a un server centrale (compresa eventualmente la marcatura temporale crittografica o la firma delle registrazioni dei log).
- Cifratura robusta e autenticazione a più fattori, in particolare per l'accesso amministrativo ai sistemi informatici, adeguata gestione delle chiavi e delle password.
- Test di vulnerabilità e di penetrazione a cadenze regolari.
- Istituire un gruppo di risposta agli incidenti di sicurezza (CSIRT) o un gruppo di risposta alle emergenze informatiche (CERT) all'interno dell'organizzazione o aderire a un CSIRT/CERT collettivo. Creare un piano di risposta agli incidenti, un piano di disaster recovery (ripristino in caso di evento catastrofico) e un piano di continuità operativa e assicurarsi che tali piani siano testati in modo approfondito.
- Nel valutare le contromisure, si dovrebbe riesaminare, testare e aggiornare l'analisi dei rischi.

3. ATTACCHI DI ESFILTRAZIONE DEI DATI

50. Gli attacchi che sfruttano le vulnerabilità dei servizi offerti dal titolare del trattamento a terzi su Internet, ad esempio mediante attacchi di injection (es. attacchi SQL injection, path traversal), compromissione di siti web e simili, possono assomigliare ad attacchi ransomware in quanto il rischio deriva dall'azione di un terzo non autorizzato, ma mirano generalmente a copiare, esfiltrare e utilizzare dati personali per fini dolosi. Si tratta quindi principalmente di violazioni della riservatezza e, eventualmente, anche dell'integrità dei dati. Allo stesso tempo, se il titolare del trattamento è a conoscenza delle caratteristiche di questo tipo di violazioni, vi sono numerose misure che possono ridurre considerevolmente il rischio di un attacco efficace.

3.1 CASO N. 05: ESFILTRAZIONE DEI DATI DELLE DOMANDE DI IMPIEGO DA UN SITO WEB

Un'agenzia per l'impiego è stata vittima di un attacco informatico, che ha inserito un codice malevolo sul suo sito web. Questo codice ha reso accessibili a soggetti non autorizzati le informazioni personali contenute nei moduli di richiesta di impiego conservati sul server web. 213 di tali moduli potrebbero essere interessati, e le analisi hanno accertato che nessuna categoria particolare di dati era oggetto della violazione. Il i malware installato aveva funzionalità che consentivano all'attaccante di rimuovere qualsiasi traccia di esfiltrazione e di monitorare il trattamento effettuato sul server e di carpire dati personali. Il malware è stato individuato solo un mese dopo la sua installazione.

3.1.1 CASO N. 05 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

51. La sicurezza dell'ambiente del titolare del trattamento è estremamente importante, dal momento che la maggior parte di queste violazioni può essere evitata garantendo che tutti i sistemi siano costantemente aggiornati, che i dati sensibili siano cifrati e che le applicazioni siano sviluppate secondo elevati standard di sicurezza quali autenticazione forte, misure contro attacchi di forza bruta, "escape" (evasione) o "sanitizing" (sanificazione) "[18] degli input degli utenti, ecc. . Anche gli audit periodici di sicurezza informatica, le valutazioni delle vulnerabilità e i test di penetrazione sono necessari per individuare e correggere tali tipi di vulnerabilità. Nel caso specifico, l'impiego di strumenti di monitoraggio dell'integrità dei file nell'ambiente di produzione avrebbe potuto facilitare l'individuazione dell'iniezione del codice (un elenco delle misure consigliate figura nella sezione 3.7).
52. Nell'indagare sulla violazione, il titolare del trattamento dovrebbe sempre partire dall'identificazione della tipologia e della metodica dell'attacco, al fine di valutare le misure da adottare. Per garantire rapidità ed efficacia di tale valutazione, il titolare dovrebbe disporre di un piano di risposta agli incidenti che specifichi le misure necessarie da adottare rapidamente per assumere il controllo dell'incidente. In questo caso particolare, il tipo di violazione costituiva un fattore di incremento del rischio, in quanto non solo veniva compromessa la riservatezza dei dati, ma il soggetto infiltrato era anche in grado di apportare modifiche al sistema cosicché veniva messa in discussione anche l'integrità dei dati.
53. Si dovrebbe tenere conto della natura, della sensibilità e del volume dei dati personali colpiti dalla violazione per determinare in che misura quest'ultima abbia inciso sugli interessati. Sebbene non siano state compromesse categorie particolari di dati personali, i dati oggetto della violazione contengono importanti informazioni sulle persone che hanno compilato i moduli online e tali dati potrebbero essere utilizzati impropriamente in vari modi (marketing indesiderato, furto di identità, ecc.), per cui la gravità delle conseguenze

dovrebbe aumentare il rischio per i diritti e le libertà degli interessati[19].

3.1.2 CASO N. 05 — MISURE DI MITIGAZIONE E OBBLIGHI

54. Se possibile, una volta risolto il problema, la banca dati dovrebbe essere confrontata con quella memorizzata in un backup sicuro. Le esperienze tratte dalla violazione dovrebbero essere utilizzate per aggiornare l'infrastruttura informatica. Il titolare del trattamento dovrebbe riportare tutti i sistemi informatici interessati a uno stato pulito noto, porre rimedio alla vulnerabilità e attuare nuove misure di sicurezza per evitare analoghe violazioni dei dati in futuro, ad esempio controlli di integrità dei file e audit di sicurezza. Se i dati personali sono stati non solo esfiltrati, ma anche cancellati, il titolare del trattamento deve intraprendere un'azione sistematica per ripristinare i dati personali nello stato in cui si trovavano prima della violazione. Potrebbe essere necessario applicare backup completi, modifiche incrementali ed eventualmente ripetere il trattamento dall'ultimo backup incrementale, il che richiede che il titolare sia in grado di replicare le modifiche apportate dopo l'ultimo backup. Ciò potrebbe necessitare che il titolare del trattamento disponga di un sistema progettato per conservare i file di input giornalieri nel caso in cui questi debbano essere nuovamente elaborati; tutto ciò richiede una tecnica robusta di memorizzazione e un'adeguata politica di conservazione prolungata dei dati.

55. Alla luce di quanto precede, poiché la violazione può comportare un rischio elevato per i diritti e le libertà delle persone fisiche, gli interessati dovrebbero esserne informati (articolo 34, paragrafo 1), il che significa naturalmente che anche le autorità di controllo competenti dovrebbero essere coinvolte attraverso una notifica di violazione dei dati. Documentare la violazione è obbligatorio ai sensi dell'articolo 33, paragrafo 5, del regolamento generale sulla protezione dei dati e facilita la valutazione del caso specifico.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	√	√

3.2 CASO N. 06: ESFILTRAZIONE DA UN SITO WEB DI PASSWORD SOTTOPOSTE AD HASHING

Una vulnerabilità SQL Injection è stata sfruttata per accedere a un database sul server di un sito web dedicato alla cucina. Agli utenti è stato consentito di scegliere solo pseudonimi arbitrari come nomi utente. È stato scoraggiato l'uso di indirizzi di posta elettronica a tal fine.

Le password memorizzate nella banca dati sono state sottoposte ad hashing con un algoritmo robusto e il salt non è stato compromesso. Dati interessati: password hashed di 1.200 utenti. Per motivi di sicurezza, il titolare del trattamento ha informato gli interessati della violazione tramite posta elettronica e ha chiesto loro di modificare le password, soprattutto se la stessa password è stata utilizzata per altri servizi.

3.2.1 CASO N. 06 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

56. In questo caso particolare, la riservatezza dei dati è compromessa, ma le password nel database sono state sottoposte ad hashing con un metodo conforme allo stato dell'arte, il che ridurrebbe il rischio per quanto riguarda la natura, la sensibilità e il volume dei dati personali. Il caso non presenta rischi per i diritti e le libertà degli interessati.
57. Inoltre, non sono state compromesse le informazioni di contatto (ad esempio indirizzi di posta elettronica o numeri di telefono) degli interessati, il che significa che non vi è alcun rischio significativo per gli interessati di essere oggetto di tentativi di frode (ad esempio, messaggi di posta elettronica di phishing o telefonate e SMS fraudolenti). Non sono state coinvolte categorie particolari di dati personali.
58. Alcuni nomi utente potrebbero essere considerati dati personali, ma la materia trattata dal sito web non genera connotazioni negative. Tuttavia, si deve osservare che la valutazione del rischio può essere diversa[20], se la natura del sito web e i dati consultati possono rivelare categorie particolari di dati personali (ad esempio il sito web di un partito politico o di un sindacato). L'uso di tecniche di cifratura conformi allo stato dell'arte potrebbe attenuare gli effetti negativi della violazione. Consentire un numero limitato di tentativi di login impedirà il successo degli attacchi di forza bruta sul login, riducendo in larga misura i rischi generati da i attaccanti che già conoscono i nomi utente.

3.2.2 CASO N. 06 — MISURE DI MITIGAZIONE E OBBLIGHI

59. In alcuni casi la comunicazione agli interessati potrebbe essere considerata un fattore di mitigazione del rischio, dal momento che anche gli interessati sono in grado di adottare le misure necessarie per evitare ulteriori danni derivanti dalla violazione, ad esempio modificando la loro password. In questo caso, la comunicazione non era obbligatoria, ma in molti casi può essere considerata una buona pratica.
60. Il titolare del trattamento dovrebbe correggere la vulnerabilità e implementare nuove misure di sicurezza per evitare in futuro analoghe violazioni dei dati, ad esempio attraverso audit sistematici di sicurezza sul sito web.
61. La violazione dovrebbe essere documentata conformemente all'articolo 33, paragrafo 5, ma non è necessaria alcuna notifica o comunicazione.

62. Inoltre, è fortemente consigliabile comunicare agli interessati una violazione che riguardi password anche se le password sono state memorizzate utilizzando un hash con l'impiego di salt attraverso un algoritmo conforme allo stato dell'arte. È preferibile utilizzare metodi di autenticazione che evitino la necessità di trattare password lato server. Gli interessati dovrebbero avere la possibilità di adottare misure adeguate per quanto riguarda le proprie password.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	X	X

3.3 CASO N. 07: ATTACCO DEL TIPO CREDENTIAL *STUFFING* SU UN SITO WEB BANCARIO

Una banca ha subito un attacco informatico contro uno dei suoi siti web di servizi bancari online. L'attacco mirava a elencare tutti gli identificativi utente di accesso possibili utilizzando una banale password fissa. Le password sono composte da 8 cifre. A causa di vulnerabilità del sito web, in alcuni casi l'autore dell'attacco ha potuto accedere a informazioni riguardanti gli interessati (nome, cognome, sesso, data e luogo di nascita, codice fiscale, codici di identificazione dell'utente), anche se la password utilizzata non era corretta o il conto bancario non era più attivo. Ciò ha interessato circa 100.000 soggetti. Fra questi, l'autore dell'attacco si è connesso con successo a circa 2.000 account che utilizzavano la password banale da questi processata . Successivamente il titolare del trattamento è stato in grado di individuare tutti i tentativi illegittimi di log-on. Il titolare ha potuto verificare che, in base ai controlli antifrode, su tali account non è stata effettuata alcuna transazione durante l'attacco. La banca era a conoscenza della violazione dei dati in quanto il suo centro operativo di sicurezza ha individuato un numero elevato di richieste di login dirette verso il sito web. In risposta, il titolare del trattamento ha disattivato temporaneamente la possibilità di connettersi al sito web e ha forzato il cambio password degli account compromessi. Il titolare ha comunicato la violazione solo agli utenti con account compromessi, ossia agli utenti le cui password sono state compromesse o i cui dati sono stati divulgati.

3.3.1 CASO N. 07 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

63. È importante ricordare che i titolari che trattano dati di natura estremamente personale[21] hanno maggiori responsabilità in termini di garanzia di un'adeguata sicurezza dei dati, ad esempio predisponendo un centro operativo

di sicurezza e attuando altre misure di prevenzione, rilevamento e risposta agli incidenti. Il mancato rispetto di questi standard più elevati comporterà certamente l'adozione di misure più severe durante l'indagine di un'autorità di controllo.

64. La violazione riguarda dati finanziari che vanno al di là dell'identità e delle informazioni identificative dell'utente, il che la rende particolarmente grave. Il numero di persone interessate è elevato.

65. Il fatto che una violazione possa verificarsi in un ambiente così sensibile segnala la presenza di notevoli lacune della sicurezza dei dati nel sistema del titolare del trattamento e può essere un indicatore della necessità di un riesame e di un aggiornamento delle misure in questione, in linea con gli articoli 24 (1), 25 (1) e 32 (1) del GDPR. I dati violati consentono l'identificazione univoca degli interessati e contengono altre informazioni su di essi (tra cui sesso, data e luogo di nascita); inoltre possono essere utilizzati dall'autore dell'attacco per ricavare le password dei clienti o per condurre una campagna di phishing mirata ai clienti della banca.

66. Per questi motivi, la violazione dei dati è stata ritenuta suscettibile di comportare un rischio elevato per i diritti e le libertà di tutti gli interessati[22]. Pertanto, è ipotizzabile il verificarsi di un danno materiale (ad esempio una perdita finanziaria) e immateriale (ad esempio furto d'identità o frode) in conseguenza della violazione.

3.3.2 CASO N. 07 — MISURE DI MITIGAZIONE E OBBLIGHI

67. Le misure del titolare del trattamento menzionate nella descrizione del caso sono adeguate. A seguito della violazione, ha inoltre corretto la vulnerabilità del sito web e ha adottato altre misure per prevenire analoghe violazioni dei dati in futuro, come l'aggiunta di un'autenticazione a due fattori al sito web interessato e il passaggio a un'autenticazione forte del cliente.

68. In questo scenario la documentazione della violazione a norma dell'articolo 33, paragrafo 5, del GDPR e la notifica all'autorità di controllo non sono lasciate alla discrezione del titolare. Inoltre, il titolare del trattamento dovrebbe informare tutti i 100.000 interessati (compresi gli interessati i cui account non sono stati compromessi) a norma dell'articolo 34 del GDPR.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	√	√

3.4 MISURE ORGANIZZATIVE E TECNICHE PER PREVENIRE/MITIGARE GLI EFFETTI DEGLI ATTACCHI DI HACKER

69. Come nel caso degli attacchi ransomware, indipendentemente dall'esito e dalle conseguenze dell'attacco, i titolari sono tenuti a riconsiderare le misure di sicurezza dei sistemi informativi in casi analoghi.

70. Misure consigliate[23]:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

- Cifratura e gestione delle chiavi conformi allo stato dell'arte, in particolare quando si trattano password, dati sensibili o finanziari. L'hashing e l'utilizzo di salt crittografici sono sempre preferibili in caso di informazioni riservate (password) rispetto alla cifratura delle password. È preferibile utilizzare metodi di autenticazione che evitino la necessità di trattare password lato server.
- Aggiornamento del sistema (software e firmware). Garantire l'applicazione di tutte le misure di sicurezza informatica, garantirne l'efficacia e mantenerle regolarmente aggiornate quando il trattamento o le circostanze cambiano o evolvono. Per essere in grado di dimostrare la conformità all'articolo 5, paragrafo 1, lettera f), a norma dell'articolo 5, paragrafo 2, del GDPR, il titolare del trattamento dovrebbe conservare un registro di tutti gli aggiornamenti effettuati, compreso il momento in cui sono stati applicati.
- Uso di metodi di autenticazione forte quali autenticazione a due fattori e server di autenticazione, integrati da una politica aggiornata in materia di password.
- Gli standard sicuri di sviluppo comprendono l'applicazione di un filtro agli input utente (utilizzando per quanto possibile una *white list*), la sanificazione degli input utente e misure di prevenzione degli attacchi di forza bruta (come limitare il numero massimo di tentativi ripetuti). L'impiego di Web Application Firewall (WAF - firewall per le applicazioni web) può supportare l'implementazione efficace di questa tecnica.
- Politiche robuste per i privilegi utente e la gestione del controllo degli accessi.
- Uso di sistemi di protezione, di rilevamento delle intrusioni e di difesa perimetrale adeguati, aggiornati, efficaci e integrati.
- Audit sistematici della sicurezza informatica e valutazioni delle vulnerabilità (test di penetrazione).
- Revisioni e test periodici per garantire l'utilizzabilità dei backup al fine di ripristinare i dati la cui integrità o disponibilità siano state compromesse.
- Nessun identificativo di sessione nell'URL in chiaro.

4. FONTI DI RISCHIO INTERNE LEGATE AL FATTORE UMANO

71. Occorre evidenziare il ruolo dell'errore umano nelle violazioni dei dati per-

sonali a causa della sua frequenza. Poiché queste violazioni possono essere sia intenzionali che accidentali, è molto difficile per i titolari del trattamento individuare le vulnerabilità e adottare misure per evitarle. La Conferenza internazionale delle autorità per la protezione dei dati e la privacy ha riconosciuto l'importanza di affrontare tali fattori umani e ha adottato, nell'ottobre 2019, una risoluzione concernente il ruolo dell'errore umano nelle violazioni dei dati personali[24]. La risoluzione sottolinea la necessità di adottare misure di salvaguardia adeguate al fine di prevenire gli errori umani e fornisce un elenco non esaustivo di garanzie e approcci.

4.1 CASO N. 08: ESFILTRAZIONE DI DATI AZIENDALI DA PARTE DI UN DIPENDENTE

Durante il suo periodo di preavviso, il dipendente di una società copia i dati aziendali dalla banca dati della società. Il dipendente è autorizzato ad accedere ai dati solo per svolgere le sue mansioni. Vari mesi dopo aver cessato il lavoro alle dipendenze della società, utilizza i dati così ottenuti (dati di contatto di base) per alimentare un nuovo trattamento dei dati per il quale è il titolare, al fine di contattare i clienti della società e invitarli a rivolgersi alla sua nuova impresa.

4.1.1 CASO N. 08 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

72. Nel caso di specie non sono state adottate misure preventive per impedire al dipendente di copiare i dati di contatto della clientela della società, in quanto il dipendente aveva bisogno legittimamente di accedere – e di fatto accedeva – a tali informazioni per le sue mansioni. Poiché la gestione dei clienti richiede nella maggior parte dei casi un qualche tipo di accesso dei dipendenti ai dati personali, tali violazioni possono essere le più difficili da prevenire. Limitando la portata dell'accesso si rischia di limitare il lavoro che il dipendente è in grado di svolgere. Tuttavia, politiche di accesso ben concepite e un controllo costante possono contribuire a prevenire tali violazioni.
73. Come di consueto, durante la valutazione del rischio devono essere presi in considerazione il tipo di violazione e la natura, la sensibilità e il volume dei dati personali interessati. Queste violazioni sono generalmente violazioni della riservatezza, in quanto la banca dati è solitamente lasciata intatta e il suo contenuto è "semplicemente" copiato in vista di un ulteriore utilizzo. La quantità di dati interessati è solitamente bassa o media. In questo caso particolare non sono state coinvolte categorie particolari di dati personali, il dipendente aveva bisogno soltanto delle informazioni di contatto dei clienti per essere in grado di contattarli dopo aver lasciato la società. Pertanto, i dati in questione non sono sensibili.
74. Sebbene l'unico obiettivo dell'ex-dipendente che ha copiato in modo fraudolento i dati possa consistere nell'ottenere le informazioni di contatto della

clientela della società per i propri scopi di natura commerciale, il titolare del trattamento non può considerare basso il rischio per gli interessati poiché non dispone di alcuna certezza sulle intenzioni del dipendente. Pertanto, sebbene le conseguenze della violazione possano limitarsi all'esposizione alle attività di autopromozione svolte dall'ex-dipendente, non è escluso un ulteriore e più grave abuso dei dati copiati, a seconda della finalità del trattamento messo in atto dall'ex-dipendente[25].

4.1.2 CASO N. 08 — MISURE DI MITIGAZIONE E OBBLIGHI

75. Nel caso di specie è difficile mitigare gli effetti negativi della violazione. Potrebbe essere necessario avviare un'azione legale immediata per impedire all'ex-dipendente di utilizzare impropriamente e diffondere ulteriormente i dati. In seconda battuta, l'obiettivo dovrebbe essere quello di evitare situazioni analoghe in futuro. Il titolare del trattamento potrebbe chiedere un'ingiunzione che imponga all'ex-dipendente di astenersi dall'utilizzo dei dati, ma le probabilità che ciò risulti efficace sono, nella migliore delle ipotesi, opinabili. Possono essere utili misure tecniche adeguate, come l'impossibilità di copiare o scaricare dati su dispositivi amovibili.
76. Non esiste una soluzione unica per tutti i casi di questo tipo, ma un approccio sistematico può contribuire a prevenirli. Ad esempio, l'impresa può prendere in considerazione, ove possibile, la limitazione degli accessi per i dipendenti che hanno segnalato l'intenzione di licenziarsi, oppure prevedere log degli accessi in modo da registrare e segnalare ogni accesso indesiderato. Il contratto firmato con i dipendenti dovrebbe includere clausole che vietino attività del genere descritto.
77. Nel complesso, poiché la violazione in questione non comporterà un rischio elevato per i diritti e le libertà delle persone fisiche, è sufficiente una notifica all'autorità di controllo. Tuttavia, informarne gli interessati potrebbe essere vantaggioso anche per il titolare del trattamento, in quanto sarebbe meglio che gli interessati ricevano la notizia della violazione dall'azienda piuttosto che apprenderla quando l'ex-dipendente cercherà di contattarli. La documentazione della violazione a norma dell'articolo 33, paragrafo 5, è un obbligo giuridico.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	√	X

4.2 CASO N. 09: TRASMISSIONE ACCIDENTALE DI DATI A UN TERZO FIDATO

Un agente assicurativo ha notato che — a causa dalle impostazioni difettose di un file Excel ricevuto per posta elettronica — era in grado di accedere alle informazioni relative a una ventina di clienti non appartenenti al suo portafoglio. Egli è vincolato dal segreto professionale ed è stato l'unico destinatario del messaggio di posta elettronica. L'accordo tra il titolare del trattamento e l'agente assicurativo obbliga quest'ultimo a segnalare senza ingiustificato ritardo una violazione dei dati personali al titolare stesso. Pertanto, l'agente ha immediatamente segnalato l'errore al titolare, che ha corretto il file e lo ha inviato nuovamente, chiedendo all'agente di cancellare il messaggio precedente. In base all'accordo di cui sopra, l'agente deve confermare la cancellazione per iscritto, cosa che ha fatto. Le informazioni raccolte non comprendono categorie particolari di dati personali, solo dati di contatto e dati relativi all'assicurazione stessa (tipo di assicurazione, importo). Dopo aver analizzato i dati personali interessati dalla violazione, il titolare del trattamento non ha individuato elementi particolari, sia per quanto riguarda gli interessati sia per quanto riguarda lo stesso titolare, tali da incidere sul livello di impatto della violazione.

4.2.1 CASO N. 09 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

78. In questo caso la violazione non deriva da un'azione deliberata di un dipendente, ma da un errore umano accidentale causato da disattenzione. Questo tipo di violazione può essere evitato o reso meno frequente: a) applicando programmi di formazione, istruzione e sensibilizzazione cosicché i dipendenti acquisiscano una migliore comprensione dell'importanza della protezione dei dati personali; b) riducendo lo scambio di file tramite posta elettronica, e utilizzando invece sistemi dedicati per il trattamento dei dati dei clienti; c) verificando due volte i file prima dell'invio; d) separando il momento della creazione da quello dell'invio di file.

79. La violazione riguarda solo la riservatezza dei dati, e l'integrità e l'accessibilità degli stessi non sono compromesse. La violazione dei dati riguardava solo una ventina di clienti, per cui è contenuto il volume dei dati interessati. Inoltre, non sono coinvolti dati sensibili. Il fatto che il responsabile del trattamento abbia contattato immediatamente il titolare dopo essere venuto a conoscenza della violazione dei dati può essere considerato un fattore di mitigazione del rischio. (Sarebbe da valutare anche l'eventualità che i dati siano stati trasmessi ad altri agenti assicurativi e, in caso di conferma, si dovrebbero adottare misure adeguate.) Grazie alle misure appropriate adottate successivamente alla violazione dei dati, probabilmente quest'ultima non avrà alcun impatto sui diritti e sulle libertà degli interessati.

80. Il basso numero di persone interessate, la rilevazione immediata della violazione e le misure adottate per minimizzarne gli effetti rendono il caso in questione privo di rischi.

4.2.2 CASO N. 09 — MISURE DI MITIGAZIONE E OBBLIGHI

81. Vi sono altri elementi di mitigazione del rischio nel caso in esame: l'agente è vincolato al segreto professionale; egli stesso ha segnalato il problema al titolare del trattamento e ha cancellato il file su richiesta. La sensibilizzazione ed eventualmente la previsione di ulteriori misure di controllo dei documenti contenenti dati personali potranno contribuire a evitare il ripetersi di situazioni simili in futuro.
82. Oltre a documentare la violazione a norma dell'articolo 33, paragrafo 5, non sono necessarie altre azioni.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	X	X

4.3 MISURE ORGANIZZATIVE E TECNICHE PER PREVENIRE/ATTENUARE L'IMPATTO DELLE FONTI INTERNE DI RISCHIO LEGATE AL FATTORE UMANO

83. L'applicazione congiunta delle misure indicate di seguito, in funzione delle caratteristiche specifiche del caso, dovrebbe contribuire a ridurre le probabilità di una recidiva analoga.
84. Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

- Attuazione periodica di programmi di formazione, istruzione e sensibilizzazione per i dipendenti sugli obblighi in materia di privacy e sicurezza e sulla rilevazione e la segnalazione di minacce alla sicurezza dei dati personali[26]. Messa a punto di un programma di sensibilizzazione per ricordare ai dipendenti gli errori più comuni che portano a violazioni dei dati personali e come evitarli.
- Istituzione di pratiche, procedure e sistemi solidi ed efficaci in materia di protezione dei dati e di tutela della vita privata[27].
- Valutazione delle pratiche, delle procedure e dei sistemi in materia di tutela della vita privata per garantirne l'efficacia nel tempo[28].
- Elaborazione di adeguate politiche di controllo dell'accesso e obbligo per gli utenti di rispettare le norme.
- Tecniche per forzare l'autenticazione dell'utente quando accede a dati personali sensibili.

- Disabilitazione dell'account aziendale non appena il dipendente lascia l'azienda.
- controllo dei flussi di dati insoliti tra il file server e le postazioni di lavoro dei dipendenti.
- impostazione della sicurezza dell'interfaccia I/O nel BIOS o mediante l'uso di software che controlla l'uso delle interfacce del computer (blocco o sblocco, ad esempio USB/CD/DVD, ecc.).
- revisione delle politiche in materia di accesso dei dipendenti (ad esempio, registrare l'accesso a dati sensibili chiedendo all'utente di inserire una motivazione di ordine aziendale, in modo che sia disponibile per gli audit).
- Disabilitazione dei servizi di cloud aperti.
- Vietare e impedire l'accesso a servizi di posta elettronica aperta noti.
- Disattivazione della funzione *print screen* [stampa schermata] nel sistema operativo (OS).
- Applicazione rigorosa di una politica della "scrivania sgombra" (c.d. *clean desktop*).
- Blocco automatico di tutti i computer dopo un certo periodo di inattività.
- Utilizzo di meccanismi (ad esempio token (wireless) per accedere a/aprire account bloccati) per cambi rapidi di utente in ambienti condivisi.
- Utilizzo di sistemi dedicati per la gestione dei dati personali che prevedano adeguati meccanismi di controllo dell'accesso e siano in grado di prevenire errori umani, come l'invio di comunicazioni al soggetto sbagliato. L'uso di fogli di calcolo e di altri documenti d'ufficio non è adeguato al fine di gestire i dati dei clienti.

5. SMARRIMENTO O FURTO DI DISPOSITIVI O DI DOCUMENTI CARTACEI

85. Un caso frequente è lo smarrimento o il furto di dispositivi portatili. In questi casi, il titolare del trattamento deve prendere in considerazione le circostanze del trattamento, quali le categorie dei dati conservati sul dispositivo, nonché le risorse di supporto, e le misure adottate precedentemente alla violazione per garantire un livello di sicurezza adeguato. Tutti questi elementi incidono sui potenziali impatti della violazione dei dati. La valutazione dei rischi potrebbe risultare difficile, in quanto il dispositivo non è più disponibile.

86. Questo tipo di violazione può essere classificato in tutti i casi come violazione della riservatezza. Tuttavia, se non esiste un backup per il database sottratto, può configurarsi anche una violazione della disponibilità e dell'integrità.

87. Gli scenari descritti di seguito illustrano in che modo le circostanze di cui sopra determinano la probabilità e la gravità della violazione dei dati.

5.1 CASO N. 10: FURTO DI SUPPORTI SUI QUALI SONO MEMORIZZATI DATI PERSONALI CIFRATI

A seguito di un'effrazione compiuta in un asilo, sono stati rubati due tablet. Nei tablet era installata un'app contenente dati personali sui bambini che frequentano l'asilo: nome, data di nascita, dati personali relativi alle attività educative. Sia i tablet cifrati, che erano spenti al momento dell'effrazione, sia l'app erano protetti da una password robusta. Per il titolare era prontamente ed efficacemente disponibile il back-up. Subito dopo essere venuto a conoscenza dell'effrazione, l'asilo ha inviato un comando a distanza per rimuovere il contenuto dei tablet.

5.1.1 CASO N. 10 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

88. In questo caso particolare, il titolare del trattamento ha adottato misure adeguate per prevenire e mitigare gli effetti di una potenziale violazione dei dati utilizzando la cifratura dei dispositivi, introducendo un'adeguata protezione delle password e garantendo il back-up dei dati conservati sui tablet. (Un elenco delle misure consigliate figura nella sezione 5.7).
89. Dopo essere venuto a conoscenza di una violazione, il titolare del trattamento dovrebbe valutare la fonte di rischio, i sistemi a supporto del trattamento dei dati, il tipo di dati personali coinvolti e gli impatti potenziali della violazione sulle persone interessate. La violazione dei dati sopra descritta avrebbe riguardato la riservatezza, la disponibilità e l'integrità dei dati; tuttavia, grazie alle idonee misure adottate dal titolare precedentemente e successivamente alla violazione dei dati, nessuna di tali compromissioni si è verificata.

5.1.2 CASO N. 10 — MISURE DI MITIGAZIONE E OBBLIGHI

90. La riservatezza dei dati personali sui dispositivi non è stata compromessa grazie alla protezione delle password robuste sia sui tablet che sulle app. I tablet sono stati configurati in modo tale che la l'impostazione di una password comporti la cifratura dei dati nel dispositivo. A ciò si aggiunga il tentativo del titolare di cancellare da remoto tutte le informazioni nei tablet rubati.
91. Grazie alle misure adottate, anche la riservatezza dei dati non è stata compromessa. Inoltre, il backup garantiva la costante disponibilità dei dati personali, pertanto non si sarebbe potuto verificare alcun potenziale impatto negativo.
92. Ne deriva l'improbabilità che la violazione dei dati sopra descritta comporti un rischio per i diritti e le libertà degli interessati, pertanto non occorre alcuna notifica all'autorità di controllo o agli interessati. Tuttavia, anche una violazione di questo tipo deve essere documentata, a norma dell'articolo 33, paragrafo 5.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	X	X

5.2 CASO N. 11: FURTO DI SUPPORTI SUI QUALI SONO MEMORIZZATI DATI PERSONALI NON CIFRATI

Il computer portatile di un dipendente di una società di servizi è stato rubato. Il notebook rubato conteneva nomi, cognomi, sesso, indirizzi e data di nascita di oltre 100.000 clienti. A causa dell'indisponibilità del dispositivo rubato non è stato possibile individuare se fossero interessate anche altre categorie di dati personali. L'accesso al disco rigido del notebook non era protetto da alcuna password. È possibile ripristinare i dati personali attraverso i backup giornalieri disponibili.

5.2.1 CASO N. 11 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

93. Poiché il titolare del trattamento non ha adottato alcuna misura di sicurezza, i dati personali memorizzati nel notebook rubato erano facilmente accessibili all'autore del furto o a qualsiasi altra persona che successivamente entrasse in possesso del dispositivo.
94. Questa violazione riguarda la riservatezza dei dati conservati sul dispositivo rubato.
95. In questo caso il notebook contenente i dati personali era vulnerabile in quanto non disponeva di alcuna password di protezione né di cifratura. La mancanza di misure di sicurezza di base aumenta il livello di rischio per gli interessati. Un'ulteriore criticità è rappresentata dall'identificazione degli interessati, il che aumenta anche la gravità della violazione. Il numero considerevole di persone interessate comporta un incremento del rischio; tuttavia, nella violazione non sono coinvolte categorie particolari di dati personali.
96. Nel corso della valutazione del rischio[29], il titolare del trattamento dovrebbe prendere in considerazione le potenziali conseguenze e gli effetti negativi della violazione della riservatezza. A causa della violazione, gli interessati possono subire furti di identità sulla base dei dati disponibili nel notebook sottratto, per cui il rischio è da ritenersi elevato.

5.2.2 CASO N. 11 — MISURE DI MITIGAZIONE E OBBLIGHI

97. La cifratura del dispositivo e l'uso della protezione di una password robusta

del database memorizzato nel dispositivo avrebbero potuto impedire che la violazione dei dati comportasse un rischio per i diritti e le libertà degli interessati.

98. Alla luce di tali circostanze, è necessaria la notifica all'autorità di controllo competente nonché la comunicazione agli interessati.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	√	√

5.3 CASO N. 12 – FURTO DI FASCICOLI CARTACEI CONTENENTI DATI SENSIBILI

Un registro cartaceo è stato rubato da un centro per la riabilitazione dalle tossicodipendenze. Il registro conteneva dati identificativi e sanitari di base relativi ai pazienti del centro. I dati erano memorizzati solo sul supporto cartaceo e i medici che trattavano i pazienti non dispongono di un backup. Il registro non era conservato in un cassetto chiuso a chiave né in una stanza chiusa a chiave; il titolare non aveva previsto politiche per il controllo degli accessi né altre misure a protezione della documentazione cartacea.

5.3.1 CASO N. 12 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

99. Poiché il titolare del trattamento dei dati non ha adottato alcuna misura di sicurezza, i dati personali conservati nel registro erano facilmente accessibili alla persona che lo ha trovato. Inoltre, la natura dei dati personali conservati nel registro rende la mancanza di un backup un fattore di rischio molto grave.

100. Questo caso esemplifica una violazione dei dati ad alto rischio. A causa della mancanza di adeguate precauzioni a, sono andati perduti dati sanitari sensibili a norma dell'articolo 9, paragrafo 1, del GDPR. Poiché in questo caso si trattava di una categoria particolare di dati personali, i rischi potenziali per gli interessati sono maggiori, e tale circostanza deve essere tenuta in considerazione anche dal titolare del trattamento nell'effettuare la valutazione del rischio[30].

101. La violazione riguarda la riservatezza, la disponibilità e l'integrità dei dati personali in questione. La violazione compromette la segretezza del rapporto medico-paziente, e terzi non autorizzati possono accedere alle informazioni sanitarie riguardanti i pazienti, il che può avere gravi ripercussioni sulla loro vita. La violazione della disponibilità può anche compromettere la continuità delle cure prestate. Non potendosi escludere la modifica/can-

cellazione di parti del contenuto del registro, risulta compromessa anche l'integrità dei dati personali.

5.3.2 CASO N. 12 — MISURE DI MITIGAZIONE E OBBLIGHI

102. In fase di valutazione delle misure di salvaguardia dovrebbe essere presa in considerazione anche la natura del supporto utilizzato. Poiché il registro dei pazienti era un documento fisico, la sua protezione avrebbe dovuto essere organizzata in modo diverso rispetto a un dispositivo elettronico. La pseudonimizzazione dei nomi dei pazienti, la conservazione del registro in un locale protetto e in un cassetto o una stanza chiusi a chiave, e un adeguato controllo degli accessi che prevedesse l'autenticazione al momento dell'accesso avrebbero potuto impedire la violazione dei dati.

103. La violazione dei dati di cui sopra può avere gravi ripercussioni sugli interessati; di conseguenza, la notifica dell'autorità di controllo e la comunicazione della violazione agli interessati sono obbligatorie.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	√	√

5.4 MISURE ORGANIZZATIVE E TECNICHE PER PREVENIRE/ATTENUARE LE CONSEGUENZE DELLA PERDITA O DEL FURTO DI DISPOSITIVI

104. L'applicazione congiunta delle misure indicate di seguito, in funzione delle caratteristiche specifiche del caso, dovrebbe contribuire a ridurre la probabilità del ripetersi di incidenti analoghi.

105. Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

- Attivare sistemi di cifratura del dispositivo (come BitLocker, Veracript o DM-Crypt).
- Utilizzare un codice di accesso/password su tutti i dispositivi. Cifrare tutti i dispositivi elettronici mobili prevedendo l'inserimento di una password complessa per la decifratura.
- Utilizzare l'autenticazione a più fattori.
- Attivare le funzionalità dei dispositivi ad alta mobilità che ne consentono la localizzazione in caso di perdita o smarrimento.

- Utilizzare software/app e localizzazione MDM (Mobile Devices Management). Utilizzare filtri antiriflesso. Chiudere tutti i dispositivi incustoditi.
- Se possibile e opportuno per il trattamento dei dati in questione, salvare i dati personali non su un dispositivo mobile, ma su un server centrale di back-end.
- Se la postazione di lavoro è collegata alla LAN aziendale, eseguire un backup automatico dalle cartelle di lavoro, a condizione che sia ineludibile che i dati personali siano ivi conservati.
- Utilizzare una VPN sicura (ad esempio, che richieda un secondo fattore di autenticazione separato per stabilire una connessione sicura) per collegare i dispositivi mobili ai server back-end.
- Fornire dispositivi di blocco fisico ai dipendenti per consentire loro di mettere fisicamente in sicurezza i dispositivi mobili che utilizzano quando rimangono incustoditi.
- Corretta regolamentazione dell'uso del dispositivo al di fuori dell'azienda.
- Corretta regolamentazione dell'uso dei dispositivi all'interno dell'azienda.
- Utilizzare software/app MDM (Mobile Devices Management) e attivare la funzione wipe da remoto.
- Utilizzare una gestione centralizzata dei dispositivi con diritti minimi per l'installazione di software da parte degli utenti finali.
- Installare controlli di accesso fisico.
- Evitare di conservare informazioni sensibili in dispositivi mobili o dischi rigidi. Se è necessario accedere al sistema interno dell'impresa, si dovrebbero utilizzare canali sicuri come indicato in precedenza.

6. ERRATO INVIO DI CORRISPONDENZA

106. Anche in questo caso la fonte di rischio è un errore umano interno, ma nessun atto doloso ha portato alla violazione. È il risultato di una disattenzione. Ben poco può fare il titolare del trattamento una volta che la violazione si sia verificata, pertanto la prevenzione in questi casi è ancora più importante.

6.1 CASO N. 13: ERRORE NELLA CORRISPONDENZA POSTALE

Due ordini per l'acquisto di calzature sono stati evasi da una società di vendita al dettaglio. A causa di un errore umano, è stata fatta confusione con le due fatture per cui sia i prodotti che le relative fatture sono stati inviati alla persona sbagliata. Ciò significa che i due clienti hanno ricevuto gli ordini l'uno dell'altro, comprese le fatture contenenti i dati personali. Dopo essere venuto a conoscenza della violazione, il titolare del trattamento ha richiamato gli ordini e li ha inviati ai destinatari corretti.

6.1.1 CASO N. 13 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

107. Le fatture contenevano i dati personali necessari per la consegna (nome, indirizzo, oltre all'articolo acquistato e il suo prezzo). È importante individuare in primo luogo come abbia potuto verificarsi l'errore umano e, se del caso, come avrebbe potuto essere evitato. Nel caso specifico, il rischio è basso, poiché non sono state coinvolte categorie particolari di dati personali o altri dati il cui abuso potrebbe avere effetti negativi rilevanti, la violazione non consegue a un errore sistemico da parte del titolare del trattamento e sono interessate solo due persone. Non sono stati rilevati effetti negativi sugli interessati.

6.1.2 CASO N. 13 — MISURE DI MITIGAZIONE E OBBLIGHI

108. Il titolare del trattamento dovrebbe prevedere la restituzione gratuita degli articoli e delle relative fatture, nonché chiedere ai destinatari errati di distruggere/cancellare tutte le eventuali copie delle fatture contenenti i dati personali dell'altro destinatario.

109. Anche se la violazione non comporta di per sé un rischio elevato per i diritti e le libertà delle persone interessate e, di conseguenza, la comunicazione agli interessati non è richiesta ai sensi dell'articolo 34 del GDPR, tale comunicazione di fatto è inevitabile in quanto è necessaria la cooperazione degli interessati per la mitigazione del rischio.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	X	X

6.2 CASO N. 14: DATI PERSONALI ALTAMENTE RISERVATI INVIATI ERRONEAMENTE PER POSTA ELETTRONICA

Il dipartimento risorse umane di una pubblica amministrazione ha inviato un messaggio di posta elettronica — sulle attività formative previste — alle persone registrate nel sistema come in cerca di occupazione. Per errore, all'e-mail è stato allegato un documento contenente tutti i dati personali di tali soggetti (nome, indirizzo e-mail, indirizzo postale, numero di previdenza sociale). Gli interessati coinvolti sono oltre 60.000. Successivamente, l'Ufficio ha contattato tutti i destinatari chiedendo loro di cancellare il messaggio precedente e di non utilizzare le informazioni in esso contenute.

6.2.1 CASO N. 14 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

110. Per l'invio di messaggi di questo genere avrebbero dovuto essere applicate regole più rigorose. Occorre prendere in considerazione l'introduzione di meccanismi di controllo supplementari.

111. Il numero di persone interessate è considerevole e il coinvolgimento del loro numero di previdenza sociale, insieme ad altri dati personali più basilari, aumenta ulteriormente il rischio, che può essere classificato come elevato[31]. Il titolare non può implementare misure tese a contenere l'eventuale diffusione dei dati da parte di uno qualsiasi dei destinatari.

6.2.2 CASO N. 14 — MISURE DI MITIGAZIONE E OBBLIGHI

112. Come indicato in precedenza, sono pochi gli strumenti utili a mitigare efficacemente i rischi di una violazione analoga. Sebbene il titolare del trattamento abbia chiesto la cancellazione del messaggio, non può costringere i destinatari a farlo e, di conseguenza, non può essere certo che essi adempiano a quanto richiesto.

113. In un caso del genere non dovrebbero esservi dubbi sulla necessità di tutte e tre le azioni indicate di seguito.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	√	√

6.3 CASO N. 15: DATI PERSONALI INVIATI PER ERRORE TRAMITE POSTA ELETTRONICA

Un elenco dei partecipanti a un corso di inglese giuridico tenuto presso un albergo e della durata di 5 giorni è inviato per errore a 15 partecipanti a un precedente e analogo corso anziché all'albergo. L'elenco contiene nomi, indirizzi di posta elettronica e preferenze alimentari dei 15 partecipanti. Solo due partecipanti hanno indicato le loro preferenze alimentari, dichiarando di essere intolleranti al lattosio. Nessuno dei partecipanti ha un'identità protetta. Il titolare del trattamento scopre l'errore subito dopo l'invio dell'elenco e ne informa i destinatari chiedendo loro di cancellare l'elenco.

6.3.1 CASO N. 15 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

114. Avrebbero dovuto essere applicate regole rigorose per l'invio di messaggi

contenenti dati personali. Occorre prendere in considerazione l'introduzione di meccanismi di controllo supplementari.

115. I rischi derivanti dalla natura, dalla sensibilità, dal volume e dal contesto dei dati personali sono bassi. I dati personali comprendono dati sensibili sulle preferenze alimentari di due dei partecipanti. Anche se l' informazione relativa all'intolleranza al lattosio è un dato sanitario, il rischio che tali dati siano utilizzati in modo dannoso dovrebbe essere considerato relativamente basso. Mentre nel caso di dati relativi alla salute si presume solitamente che la violazione possa comportare un rischio elevato per l'interessato[32], nel caso di specie non è possibile individuare il rischio che la violazione comporti danni fisici, materiali o immateriali all'interessato a causa della divulgazione non autorizzata di informazioni sull'intolleranza al lattosio. Contrariamente ad altre preferenze alimentari, l'intolleranza al lattosio non può di norma essere collegata a convinzioni religiose o filosofiche. Anche la quantità di dati violati e il numero di interessati coinvolti sono molto bassi.

6.3.2 CASO N. 15 — MISURE DI MITIGAZIONE E OBBLIGHI

116. In sintesi, si può affermare che la violazione non ha avuto effetti significativi sugli interessati. Il fatto che il titolare del trattamento abbia contattato immediatamente i destinatari dopo essere venuto a conoscenza dell'errore può essere considerato un fattore di mitigazione.

117. Se un messaggio di posta elettronica è inviato a un destinatario errato/non autorizzato, si raccomanda al titolare del trattamento di inviare un'e-mail di follow-up, in copia nascosta, ai destinatari non corretti, scusandosi per l'errore, invitando a cancellare l'e-mail inviata erroneamente e informando i destinatari che non hanno il diritto di utilizzare ulteriormente gli indirizzi di posta elettronica loro comunicati.

118. Alla luce delle circostanze descritte, era improbabile che la violazione dei dati comportasse un rischio per i diritti e le libertà degli interessati, pertanto non si è resa necessaria alcuna notifica all'autorità di controllo o agli interessati. Tuttavia, anche una violazione dei dati di questo tipo deve essere documentata a norma dell'articolo 33, paragrafo 5.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	X	X

6.4 CASO N. 16: ERRORE NELL'INVIO DI CORRISPONDENZA POSTALE

Un gruppo assicurativo offre assicurazioni auto. A tal fine, invia per posta aggiornamenti periodici sulle prestazioni assicurative. Oltre al nome e all'indirizzo dell'assicurato, la lettera contiene la targa del veicolo in chiaro, gli importi del premio assicurativo per l'anno in corso e per quello successivo, il chilometraggio annuo approssimativo e la data di nascita dell'assicurato. Non sono inclusi dati sanitari ai sensi dell'articolo 9 del GDPR, né dati relativi ai pagamenti (coordinate bancarie) o dati economici e finanziari.

Le lettere sono imbustate automaticamente. A causa di un errore meccanico, due lettere destinate a contraenti diversi sono inserite in una stessa busta e inviate per posta ordinaria a uno dei due. Il contraente apre la lettera a casa e legge la lettera a lui correttamente indirizzata nonché quella erroneamente consegnata e indirizzata a un diverso contraente.

6.4.1 CASO N. 16 — MISURE IN ESSERE E VALUTAZIONE DEL RISCHIO

119. La lettera erroneamente consegnata contiene il nome, l'indirizzo, la data di nascita, il numero di immatricolazione in chiaro del veicolo e la classe attribuita per il premio assicurativo dell'anno in corso e dell'anno successivo. Gli effetti sulla persona interessata devono ritenersi di media entità, in quanto sono comunicate a una persona non autorizzata informazioni non accessibili al pubblico, quali la data di nascita o i numeri di immatricolazione in chiaro dei veicoli, nonché i dettagli relativi all'aumento del premio assicurativo. La probabilità di un uso improprio di questi dati è da valutarsi tra bassa e media. Tuttavia, mentre molti destinatari probabilmente cestineranno la lettera ricevuta per errore, non si può escludere del tutto che, in determinati casi, la lettera sia pubblicata sui social network o che l'assicurato sia contattato.

6.4.2 CASO N. 16 — MISURE DI MITIGAZIONE E OBBLIGHI

120. Il titolare del trattamento deve chiedere che, a sue spese, gli sia reinviato il documento originale. Inoltre, dovrebbe informare il destinatario errato del fatto che non può utilizzare in modo improprio le informazioni cui ha avuto accesso.

121. Probabilmente non sarà mai possibile prevenire del tutto errori di spedizione in una postalizzazione massiva effettuata in forma completamente automatizzata. Tuttavia, se tali errori avvengono con una certa frequenza, è necessario verificare se i dispositivi di imbustamento siano impostate e sottoposte a manutenzione in modo corretto o se vi siano altri problemi di natura sistemica alla base della violazione.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	√	X

6.5 MISURE ORGANIZZATIVE E TECNICHE PER PREVENIRE/ATTENUARE GLI EFFETTI DI UN'ERRATA POSTALIZZAZIONE

122. L'applicazione congiunta delle misure indicate di seguito, in funzione delle caratteristiche specifiche del caso, dovrebbe contribuire a ridurre le probabilità del ripetersi di eventi analoghi.

123. Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione.)

- Definizione di standard specifici — che non lascino spazi all'interpretazione — per l'invio di lettere/e-mail.
- Formazione adeguata del personale sull'invio di lettere/e-mail.
- Quando si inviano messaggi di posta elettronica a più destinatari, questi sono inseriti nel campo "Ccn" per impostazione predefinita.
- Necessità di una conferma supplementare prima di inviare messaggi di posta elettronica a più destinatari senza inserirli nel campo "Ccn".
- Applicazione del principio del doppio livello di controllo.
- Inserimento automatico anziché manuale dei recapiti, con dati estratti da una banca dati disponibile e aggiornata; il sistema di inserimento automatico dovrebbe essere riesaminato periodicamente per verificare eventuali errori nascosti e impostazioni errate.
- Applicazione della funzionalità di invio ritardato (che consente di cancellare/modificare il messaggio entro un determinato periodo di tempo dopo aver premuto il pulsante "Invio").
- Disabilitazione del completamento automatico quando si digitano indirizzi e-mail.
- Sessioni di sensibilizzazione sugli errori più comuni che generano una violazione dei dati personali.
- Sessioni di formazione e manuali sulla gestione di incidenti che generano una violazione dei dati personali, compresa l'indicazione dei soggetti da informare (coinvolgimento del responsabile della protezione dei dati).

7. ALTRI CASI — INGEGNERIA SOCIALE (*SOCIAL ENGINEERING*)

7.1 CASO N. 17: FURTO D'IDENTITÀ

Il centro di contatto di un'impresa di telecomunicazioni riceve una telefonata da una persona che si presenta come cliente. Il presunto cliente chiede alla società di modificare l'indirizzo e-mail al quale inviare le informazioni di fatturazione. L'operatore convalida l'identità del cliente chiedendo alcuni dati personali, quali definiti dalle procedure dell'impresa. Il chiamante indica correttamente il codice fiscale e l'indirizzo postale del cliente (perché ha avuto accesso a tali informazioni). Dopo la convalida, l'operatore effettua la modifica richiesta e, successivamente, le informazioni di fatturazione sono inviate al nuovo indirizzo e-mail. La procedura non prevede alcuna notifica al precedente contatto e-mail. Il mese successivo il cliente legittimo contatta la società, chiedendo perché non riceva la fattura al suo indirizzo di posta elettronica, e nega qualsiasi richiesta da parte sua di modificare l'email di contatto. La società si rende conto che le informazioni sono state inviate a un utente illegittimo e annulla la modifica.

7.1.1 CASO N. 17 — VALUTAZIONE DEL RISCHIO, MISURE DI MITIGAZIONE E OBBLIGHI

124. Questo caso ben esemplifica l'importanza delle misure preventive. La violazione presenta un elevato livello di rischio33, in quanto i dati di fatturazione possono fornire informazioni sulla vita privata dell'interessato (ad esempio, abitudini, contatti) e potrebbero causare danni materiali (ad esempio stalking, rischio per l'integrità fisica). I dati personali ottenuti durante l'attacco possono essere utilizzati anche per facilitare l'acquisizione di account all'interno della specifica organizzazione o per testare ulteriori misure di autenticazione in altre organizzazioni. Tenuto conto di tali rischi, la soglia di "adeguatezza" delle misure di autenticazione dovrebbe essere fissata a un livello elevato in rapporto alla natura dei dati personali cui è possibile accedere una volta effettuata l'autenticazione.
125. Di conseguenza, sono necessarie sia una notifica all'autorità di controllo sia una comunicazione all'interessato da parte del titolare del trattamento.
126. È chiaro che il processo di convalida preventiva del cliente necessita di perfezionamenti, alla luce di questo caso. I metodi utilizzati per l'autenticazione non erano sufficienti. La parte malintenzionata è riuscita a fingere di essere l'utente legittimo utilizzando informazioni pubblicamente disponibili e altre informazioni cui aveva altrimenti accesso.5
127. Non si raccomanda l'uso di questa forma di autenticazione statica basata su elementi di conoscenza (in cui la risposta non cambia e non ci sono informazioni "segrete", come invece sarebbe nel caso di una password).
128. L'organizzazione dovrebbe invece utilizzare una forma di autenticazione altamente affidabile quanto alla dimostrazione che l'utente autenticato sia

realmente chi afferma di essere, e non altri. L'introduzione di un metodo di autenticazione a più fattori fuori banda risolverebbe il problema, ad esempio per verificare eventuali richieste di variazioni, attraverso l'invio di una richiesta di conferma al precedente indirizzo di contatto; oppure aggiungendo ulteriori domande di controllo e chiedendo informazioni presenti solo sulle fatture precedenti. Spetta al titolare del trattamento decidere quali misure introdurre, in quanto conosce meglio di chiunque altro i dettagli e le esigenze della sua operatività interna.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	√	√

7.2 CASO N. 18: ESFILTRAZIONE DI E-MAIL

Una catena di ipermercati ha rilevato, 3 mesi dopo la configurazione, che alcuni account di posta elettronica erano stati modificati attraverso la creazione di regole per cui ogni e-mail contenente determinate espressioni (ad esempio "fattura", "pagamento", "bonifico bancario", "autenticazione della carta di credito", "coordinate bancarie") veniva trasferita in una cartella non utilizzata e trasmessa anche a un indirizzo di posta elettronica esterno. Inoltre, a quella data, era già stato commesso un attacco di ingegneria sociale, vale a dire che l'attaccante, che fingeva di essere un fornitore, aveva modificato le coordinate bancarie di tale fornitore sostituendovi le proprie. Infine, a quella data, erano state inviate diverse fatture false che includevano i nuovi dati relativi alle coordinate bancarie. Il sistema di monitoraggio della piattaforma di posta elettronica aveva segnalato, in ultima istanza, un problema sulle cartelle. La società non è stata in grado di individuare in che modo l'attaccante fosse riuscito ad accedere agli account di posta elettronica, ma ha ritenuto che attraverso un'email infetta fosse avvenuto l'accesso al gruppo di utenti incaricati dei pagamenti.

A seguito della trasmissione di e-mail contenenti determinate parole-chiave, l'attaccante ha ricevuto informazioni su 99 dipendenti: nome e salario riferito a uno specifico mese per 89 soggetti; nome, stato civile, numero di figli, retribuzione, ore di lavoro e altre informazioni sulla retribuzione di 10 dipendenti il cui contratto era terminato. Il titolare ha comunicato la violazione soltanto ai 10 dipendenti appartenenti a quest'ultimo gruppo.

7.2.1 CASO N. 18 — VALUTAZIONE DEL RISCHIO, MISURE DI MITIGAZIONE E OBBLIGHI

129. Anche se l'attaccante non mirava probabilmente a raccogliere dati perso-

nali, la violazione potrebbe comportare sia un danno materiale (ad esempio, perdite finanziarie) che un danno immateriale (ad esempio furto o usurpazione di identità), e i dati potrebbero essere utilizzati per facilitare altri attacchi (ad esempio phishing); pertanto, la violazione potrebbe comportare un rischio elevato per i diritti e le libertà delle persone fisiche e dovrebbe essere comunicata a tutti i 99 dipendenti e non solo ai 10 dei quali sono state divulgate le retribuzioni.

130. Una volta venuto a conoscenza della violazione, il titolare del trattamento ha forzato la modifica della password per gli account compromessi, ha bloccato l'invio di e-mail all'account dell'attaccante, ha informato il fornitore del servizio di posta elettronica utilizzato dall'autore dell'attacco in merito alle azioni compiute da quest'ultimo, ha rimosso le regole stabilite dall'attaccante e perfezionato le segnalazioni del sistema di monitoraggio così da generare una segnalazione non appena venga creata una regola automatica. In alternativa, il titolare del trattamento potrebbe eliminare il diritto degli utenti di stabilire regole sull'inoltro dei messaggi di posta elettronica, prevedendo la necessità di un intervento del team del servizio informatico su specifica richiesta, oppure potrebbe introdurre una politica in base alla quale gli utenti dovrebbero verificare e comunicare le regole stabilite sui loro account una volta alla settimana o con maggiore frequenza, nei settori che trattano dati finanziari.

131. Il fatto che una violazione abbia potuto verificarsi e sfuggire al rilevamento per un periodo così prolungato, e la circostanza per cui, se la violazione fosse proseguita, le tecniche di ingegneria sociale avrebbero consentito di modificare un volume di dati ancora più consistente, evidenziano notevoli criticità nel sistema di sicurezza informatica del titolare del trattamento. Tali criticità dovrebbero essere affrontate senza indugio, ad esempio rivedendo le procedure automatizzate e le verifiche dei cambiamenti, le misure di rilevazione degli incidenti e di risposta agli incidenti. I titolari del trattamento di dati sensibili, informazioni finanziarie, ecc. hanno maggiori responsabilità nel garantire un'adeguata sicurezza dei dati.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
√	√	√

NOTE

[1] I riferimenti agli "Stati membri" nel presente documento sono da intendersi come riferimenti agli "Stati membri del SEE".

[2] COM (2020) 264 final del 24 giugno 2020.

[3] WP29 WP250 rev.1, 6 febbraio 2018, Linee guida sulla notifica delle violazioni dei dati personali a norma del regolamento 2016/679 — approvate dal comitato europeo per la protezione dei dati, https://ec.europa.eu/newsroom/article29/item-detail.cfm7item id = 612052.

[4] WP29 WP213, 25 marzo 2014, Parere 03/2014 sulla notifica di una violazione dei dati personali, pag. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index en.htm # maincontentSec4.

[5] Cfr. le Linee guida WP 250, pag. 7. — Occorre tener conto del fatto che una violazione dei dati può riguardare una o più categorie simultaneamente.

[6] Articolo 33, paragrafo 5, del GDPR.

[7] Articolo 33, paragrafo 1, del GDPR.

[8] Articolo 34, paragrafo 1, del GDPR.

[9] Articolo 33, paragrafo 4, del GDPR.

[10] Per orientamenti sui trattamenti "che possono comportare un rischio elevato", si veda il gruppo di lavoro A29 "Guidelines on Data Protection Impact Assessment (DPIA) and determining if processing is likely to be a high risk" (Linee guida sulla valutazione d'impatto sulla protezione dei dati e sulla determinazione della probabilità che il trattamento possa comportare un rischio elevato) ai fini del regolamento 2016/679, WP248 rev. 01, approvato dall'EDPB, https://ec.europa.eu/newsroom/article29/items/611236, pag. 9.

[11] Dal punto di vista tecnico, la cifratura dei dati comporta l' "accesso" ai dati originali e, nel caso di ransomware, la cancellazione dei dati originali — il codice ransomware deve accedere ai dati per cifrarli e rimuovere i dati originali. L'autore di un attacco può effettuare una copia dell'originale prima dell'eliminazione, ma i dati personali non verranno sempre estratti.. Con l'avanzare delle indagini svolte dal titolare, potrebbero emergere nuove informazioni tali da modificare la suddetta valutazione. L'accesso che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata dei dati personali o un rischio per la sicurezza dell'interessato, anche in assenza di interpretazione dei dati, può essere tanto grave quanto l'accesso seguito da interpretazione dei dati personali.

[12] Le procedure di backup dovrebbero essere strutturate, coerenti e ripetibili. Esempi di procedure di backup sono il metodo 3-2-1 e il metodo grandfather-father-son. Qualsiasi metodo dovrebbe sempre essere testato per verificarne l'efficacia in termini di copertura nonché in sede di ripristino dei dati. I test dovrebbero inoltre essere ripetuti a intervalli regolari, in particolare quando intervengono cambiamenti nel trattamento o nelle sue circostanze, al fine di garantire l'integrità del sistema.

[13] Per indicazioni sulle operazioni di trattamento "che possono comportare un rischio elevato", cfr. la nota 10.

[14] Ciò dipenderà dalla complessità e dalla struttura dei dati personali. Negli scenari più complessi, il ripristino dell'integrità dei dati, la coerenza con i metadati, la garanzia della correttezza delle relazioni all'interno delle strutture di dati e il controllo dell'accuratezza dei dati possono richiedere risorse e sforzi significativi.

[15] Per indicazioni sulle operazioni di trattamento "che possono comportare un rischio elevato ", cfr. la nota 10.

[16] Il considerando 86 del regolamento generale sulla protezione dei dati spiega che "*Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta cooperazione con l'autorità di controllo, nel rispetto degli orientamenti forniti da quest'ultima o da altre autorità competenti, quali le autorità di contrasto. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione con gli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione*".

[17] Per indicazioni sulle operazioni di trattamento "*che possono comportare un rischio elevato*", cfr. la nota 10.

[18] La sanificazione degli input dell'utente è una forma di convalida degli input finalizzata ad assicurare che solo dati adegua-

tamente formattati siano inseriti in un sistema IT.

[19] Per indicazioni sulle operazioni di trattamento "*che possono comportare un rischio elevato*", cfr. la nota 10.

[20] Per indicazioni sulle operazioni di trattamento "*che possono comportare un rischio elevato*", cfr. la nota 10.

[21] Quali le informazioni degli interessati relative a metodi di pagamento come numeri di carta, conti bancari, pagamenti online, cedolini degli stipendi, estratti conto bancari, studi economici o qualsiasi altro elemento che possa rivelare informazioni economiche relative agli interessati.

[22] Per indicazioni sulle operazioni di trattamento "*che possono comportare un rischio elevato*", cfr. la nota 10.

[23] Per lo sviluppo sicuro di applicazioni web si veda anche: https://www.owasp.org/index.php/Main page.

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf

[25] Per indicazioni sulle operazioni di trattamento "*che possono comportare un rischio elevato*", cfr. la nota 10.

[26] Sezione 2) sottosezione i) della risoluzione per affrontare il ruolo dell'errore umano nelle violazioni dei dati personali.

[27] Sezione 2) sottosezione ii) della risoluzione per affrontare il ruolo dell'errore umano nelle violazioni dei dati personali.

[28] Sezione 2) sottosezione iii) della risoluzione per affrontare il ruolo dell'errore umano nelle violazioni dei dati personali.

[29] Per indicazioni sulle operazioni di trattamento "*che possono comportare un rischio elevato*", cfr. la nota 10.

[30] Per indicazioni sulle operazioni di trattamento "*che possono comportare un rischio elevato*", cfr. la nota 10.

[31] Per indicazioni sulle operazioni di trattamento "*che possono comportare un rischio elevato*", cfr. la nota 10.

[32] Cfr. le Linee guida WP 250, pag. 23.

Linee guida 02/2021 sugli assistenti vocali virtuali Versione 2.0

Adottate il 7 luglio 2021

Cronologia delle versioni

Versione 2.0	7 luglio 2021	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	9 marzo 2021	Adozione delle linee guida ai fini della consultazione pubblica per la pubblicazione

SINTESI

Un assistente vocale virtuale (AVV) è un servizio che comprende comandi vocali e li esegue ovvero agisce da intermediario con altri sistemi informatici, se necessario. Attualmente gli AVV sono disponibili nella maggior parte degli smartphone e dei tablet, nei computer tradizionali e, da qualche anno, anche come dispositivi indipendenti, ad esempio altoparlanti intelligenti.

Gli AVV fungono da interfaccia tra gli utenti e i loro dispositivi informatici e i servizi online, come i motori di ricerca o i negozi online. A causa del loro ruolo, gli AVV hanno accesso a un'enorme quantità di dati personali, compresi tutti i comandi degli utenti (ad esempio la cronologia della navigazione o delle ricerche) e tutte le risposte (ad esempio gli appuntamenti nell'agenda).

La grande maggioranza dei servizi di AVV è stata progettata da pochi progettisti specializzati. Tuttavia, gli AVV possono funzionare unitamente ad applicazioni programmate da terzi (sviluppatori di applicazioni di AVV) per fornire comandi più sofisticati.

Per poter funzionare correttamente, un AVV necessita di un'apparecchiatura terminale munita di microfoni e altoparlanti. L'apparecchiatura archivia la voce e altri dati che gli AVV attuali trasferiscono a server di AVV remoti.

I titolari del trattamento che forniscono servizi di AVV e i loro responsabili del trattamento devono pertanto tenere conto sia del RGPD[1] sia della direttiva e-privacy[2].

Le presenti linee guida individuano alcuni dei principali problemi inerenti alla conformità e propongono alle parti interessate pertinenti alcune raccomandazioni per affrontarli.

I titolari del trattamento che forniscono servizi di AVV mediante apparecchiature terminali prive di schermo devono sempre informare gli utenti ai sensi del RGPD quando impostano o installano un AVV ovvero usano un'applicazione di AVV per la prima volta. Si raccomanda pertanto ai fornitori/progettisti di AVV e agli sviluppatori di elaborare interfacce basate sulla voce per agevolare la comunicazione delle informazioni obbligatorie.

Attualmente tutti gli AVV devono avere almeno un utente registrato nel servizio. In considerazione dell'obbligo della protezione dei dati fin dalla progettazione e per impostazione predefinita, i fornitori/progettisti di AVV e gli sviluppatori dovrebbero valutare se sia opportuno avere un utente registrato per ciascuna delle loro funzionalità.

L'account utente usato da molti progettisti di AVV collega il servizio di AVV con altri servizi, come la posta elettronica o lo streaming di video. Il CEPD ritiene che i titolari del trattamento dovrebbero astenersi da tali pratiche poiché esse comportano il ricorso a informative sulla privacy lunghe e complesse, che non sarebbero conformi al principio di trasparenza sancito dal RGPD.

Le presenti linee guida prendono in considerazione le quattro finalità principali per cui gli AVV trattano dati personali: l'esecuzione di richieste, il miglioramento del modello di apprendimento automatico dell'AVV, l'identificazione biometrica e la profilazione a fini di personalizzazione dei contenuti o della pubblicità.

Nella misura in cui i dati dell'AVV sono trattati per dare esecuzione alle richieste dell'utente, ossia nella misura strettamente necessaria per fornire un servizio richiesto dall'utente, i titolari del trattamento sono esonerati dal requisito del consenso preventivo di cui all'articolo 5, paragrafo 3, della direttiva e-privacy. Per contro, il consenso previsto dall'articolo 5, paragrafo 3, della direttiva e-privacy sarebbe necessario per archiviare informazioni o avere accesso a informazioni per qualsiasi finalità diversa dall'esecuzione di una richiesta dell'utente.

Alcuni servizi di AVV conservano i dati personali fino a quando i loro utenti ne richiedono la cancellazione. Tale prassi non è in linea con il principio di limitazione della conservazione. Gli AVV dovrebbero conservare i dati soltanto per il tempo necessario a conseguire le finalità per cui i dati personali sono trattati.

Se un titolare del trattamento si accorge (ad esempio grazie a procedimenti di verifica della qualità) che vengono raccolti dati personali in modo accidentale, dovrebbe accertarsi che esista una valida base giuridica per ciascuna finalità del trattamento di tali dati. In caso contrario, i dati raccolti accidentalmente dovrebbero essere cancellati.

Gli AVV possono trattare dati di una pluralità di interessati. I fornitori/progettisti di AVV dovrebbero pertanto implementare meccanismi di controllo dell'accesso per garantire la riservatezza, l'integrità e la disponibilità dei dati personali. Tuttavia, alcuni meccanismi tradizionali di controllo dell'accesso, come le password, non sono idonei all'uso negli AVV poiché dovrebbero essere pronunciati a voce alta. Le linee guida contengono alcune considerazioni a tale proposito, tra cui una sezione specificamente dedicata al trattamento di categorie particolari di dati a fini di identificazione biometrica.

I fornitori/progettisti di AVV dovrebbero considerare che la registrazione della voce dell'utente potrebbe comprendere anche la voce o i dati di altre persone, come rumori in sottofondo che non sono necessari ai fini del servizio. Laddove possibile, i progettisti di AVV dovrebbero dunque valutare l'opportunità di applicare tecnologie in grado di filtrare i dati non necessari e garantire che sia registrata soltanto la voce dell'utente.

Nel valutare la necessità di effettuare una valutazione d'impatto sulla protezione dei dati, il CEPD reputa altamente probabile che i servizi di AVV rientrino nelle categorie e nelle condizioni per le quali è stata individuata la necessità di tale valutazione.

I titolari del trattamento che forniscono servizi di AVV dovrebbero accertarsi che gli utenti possano esercitare i propri diritti di interessati per mezzo di comandi vocali di facile esecuzione. Alla fine del procedimento i fornitori/progettisti di AVV e gli sviluppatori di applicazioni dovrebbero segnalare all'utente, mediante una comunicazione vocale, l'invio di una notifica scritta al cellulare o all'account dell'utente ovvero con qualsiasi altra modalità scelta dall'utente, che i suoi diritti sono stati presi in debita considerazione.

Indice

1 INFORMAZIONI GENERALI

2 CONTESTO TECNOLOGICO
- 2.1 Caratteristiche di base degli assistenti vocali virtuali
- 2.2 Soggetti operanti nell'ambiente dell'AVV
- 2.3 Descrizione delle fasi
- 2.4 Espressioni di attivazione
- 2.5 Frammenti vocali e apprendimento automatico

3 ELEMENTI DI PROTEZIONE DEI DATI
- 3.1 Quadro giuridico
- 3.2 Individuazione del trattamento di dati e delle parti interessate
  - 3.2.1 Trattamento dei dati personali
  - 3.2.2 Trattamento da parte dei titolari e dei responsabili del trattamento
- 3.3 Trasparenza
- 3.4 Limitazione della finalità e base giuridica
  - 3.4.1 Esecuzione delle richieste degli utenti
  - 3.4.2 Miglioramento dell'AVV mediante addestramento dei sistemi di apprendimento automatico e revisione manuale del parlato e delle trascrizioni
  - 3.4.3 Identificazione dell'utente (con dati vocali)
  - 3.4.4 Profilazione dell'utente a fini di personalizzazione dei contenuti o della pubblicità
- 3.5 Trattamento dei dati relativi a minori
- 3.6 Conservazione dei dati
- 3.7 Sicurezza
- 3.8 Trattamenti riguardanti categorie particolari di dati
  - 3.8.1 Considerazioni generali sul trattamento di categorie particolari di dati
  - 3.8.2 Considerazioni generali sul trattamento dei dati biometrici
- 3.9 Minimizzazione dei dati
- 3.10 Responsabilizzazione
- 3.11 Protezione dei dati fin dalla progettazione e per impostazione predefinita

4 Meccanismi per l'esercizio dei diritti degli interessati

4.1 Diritto di accesso
4.2 Diritto di rettifica
4.3 Diritto di cancellazione
4.4 Diritto alla portabilità dei dati personali

5 Allegato: Riconoscimento automatico del parlato, sintesi del parlato e trattamento del linguaggio naturale
5.1 Riconoscimento automatico del parlato
5.2 Trattamento del linguaggio naturale (NLP)
5.3 Sintesi del parlato

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettere e) e j), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in appresso «RGPD»),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo n. 37 dello stesso, modificato dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018[3],

visti gli articoli 12 e 22 del proprio regolamento interno,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

1. INFORMAZIONI GENERALI

1. I recenti progressi tecnologici hanno notevolmente aumentato l'accuratezza e la popolarità degli assistenti vocali virtuali (AVV). Gli AVV sono stati integrati, tra l'altro, negli smartphone, nei veicoli connessi, negli altoparlanti intelligenti e nei televisori intelligenti. Questa integrazione ha permesso agli AVV di accedere a informazioni di natura privata; se non gestiti correttamente, tali accessi potrebbero violare i diritti delle persone fisiche alla protezione dei dati e alla tutela della vita privata. Pertanto gli AVV e le apparecchiature in cui sono integrati sono stati oggetto di esame da parte di differenti autorità per la protezione dei dati.
2. L'uso di interazioni vocali comporta numerosi vantaggi: la naturalezza dell'interazione, che non richiede un apprendimento specifico da parte degli utenti, nonché la velocità dell'esecuzione del comando e l'estensione del raggio di azione, che può consentire un accesso più rapido alle informazioni. Tuttavia, fare affidamento sulle interazioni vocali comporta anche difficoltà di corretta interpretazione del messaggio a causa della variabilità del segnale audio tra altoparlanti differenti, dell'ambiente acustico, delle ambiguità linguistiche o altro ancora.
3. Nella pratica, la fluidità o la semplificazione dei compiti resta la principale motivazione del ricorso agli AVV, ad esempio per fare/rispondere a una telefonata, programmare un temporizzatore ecc. in particolare se gli utenti non possono usare le mani. La domotica è la principale applicazione suggerita dai progettisti di AVV, che si presentano come facilitatori della vita domestica proponendo uno strumento unico e facilmente attivabile da remoto che permette di semplificare l'esecuzione di vari compiti (accendere la luce, regolare il riscaldamento, abbassare le tapparelle ecc.) e di centralizzarli. Oltre all'uso personale o domestico, i comandi vocali possono rivelarsi utili anche in contesti professionali in cui è difficile maneggiare strumenti informatici e usare comandi scritti (ad esempio nel contesto di attività manifatturiere).
4. In linea teorica, i principali beneficiari dell'interfaccia vocale potrebbero essere le persone con disabilità o ridotta autonomia, per le quali l'uso di interfacce tradizionali è problematico. L'assistenza vocale virtuale può agevolare l'accesso a informazioni e risorse informatiche e promuovere così l'inclusività, dato che l'utilizzo della comunicazione vocale permette di superare le difficoltà associate alla parola scritta che alcune categorie di utenti devono affrontare.
5. Infine, anche l'ambito sanitario offre molte opportunità d'uso per gli agenti conversazionali, siano essi vocali o meno. Ad esempio, durante la pandemia di COVID-19 sono stati impiegati vari callbot per offrire una prediagnosi agli utenti che avevano telefonato. Secondo alcune previsioni, nel lungo periodo, l'intero processo di assistenza ai pazienti potrebbe essere influenzato dalle interazioni tra esseri umani e assistenti virtuali: non soltanto a fini di benessere e prevenzione, ma anche di trattamento e sostegno.
6. Gli AVV, per la maggior parte attivati per impostazione predefinita, sono già

integrati in tutti gli oltre tre miliardi di smartphone attualmente esistenti, nonché in alcuni dei sistemi operativi più ampiamente impiegati nei PC e nei laptop. Inoltre, a seguito della recente diffusione degli altoparlanti intelligenti (nel 2019 ne sono stati venduti 147 milioni[4]) gli AVV stanno entrando in milioni di case e uffici. Gli AVV attuali, tuttavia, non offrono come impostazione predefinita l'autenticazione o meccanismi di controllo dell'accesso.

7. Il presente documento mira a fornire orientamenti per l'applicazione del RGPD nel contesto degli AVV.

2. CONTESTO TECNOLOGICO

2.1 CARATTERISTICHE DI BASE DEGLI ASSISTENTI VOCALI VIRTUALI

8. Gli AVV possono essere definiti come un'applicazione software che offre capacità di dialogo orale con un utente in un linguaggio naturale.

9. Il linguaggio naturale ha una semantica che è specifica del linguaggio umano. A seconda delle caratteristiche della lingua e della diversità del lessico, la medesima istruzione può essere formulata in molti modi, mentre alcuni comandi possono sembrare simili pur riferendosi, in realtà, a due oggetti differenti. Per ovviare a queste ambiguità si ricorre spesso a meccanismi di deduzione basati, ad esempio, su quanto è stato detto in precedenza, sul momento in cui è stata data l'istruzione, sul luogo, sugli interessi della persona ecc.

10. Un AVV può essere scomposto in moduli che consentono l'esecuzione di compiti differenti: rilevamento e restituzione di suoni, trascrizione automatica del linguaggio parlato (dal linguaggio parlato al testo), trattamento automatico del linguaggio, strategie di dialogo, accesso a ontologie (serie di dati e concetti strutturati relativi a un determinato dominio) e a fonti esterne di conoscenze, generazione di linguaggio, sintesi vocale (dal testo al linguaggio parlato) e altri ancora. In concreto, l'assistente dovrebbe consentire l'interazione per compiere azioni (ad esempio «accendere la radio», «spegnere la luce») o per accedere a conoscenze (ad esempio «che tempo farà domani?», «il treno delle 7:43 è in orario?»). L'AVV funge quindi da intermediario e orchestratore con il compito di facilitare l'adempimento dei compiti dell'utente.

11. Nella pratica, un AVV non è un altoparlante intelligente, ma un altoparlante intelligente può essere munito di un assistente vocale. Capita spesso di confondere questi due dispositivi, mentre il secondo è semplicemente la materializzazione del primo. Un AVV può essere impiegato in uno smartphone, un altoparlante intelligente, un orologio connesso, un veicolo, un elettrodomestico ecc.

12. L'organizzazione del sottostante trattamento dei dati può coinvolgere numerosi modelli di flussi di informazioni. Si possono individuare tre elementi principali:

    la componente fisica: l'elemento hardware in cui è incorporato l'assistente (smartphone, altoparlante, televisore intelligente ecc.) e che è dotato di mi-

crofoni, altoparlanti e capacità di rete e informatiche (più o meno sviluppate a seconda del caso);

la componente software: la componente che implementa l'interazione uomo-macchina in senso stretto e integra i moduli per il riconoscimento vocale automatico del parlato, il trattamento del linguaggio naturale, il dialogo e la sintesi vocale; questa parte può essere gestita direttamente all'interno dell'apparecchiatura fisica, ma in molti casi è operata da remoto;

le risorse: dati esterni come banche dati di contenuti, ontologie o applicazioni professionali che forniscono conoscenze (ad esempio «dimmi che ore sono sulla costa occidentale degli Stati Uniti», «leggi le mie mail») o rendono possibile l'esecuzione concreta dell'azione richiesta (ad esempio «alza la temperatura di 1,5 °C»).

13. Gli AVV permettono di installare componenti o applicazioni di terzi per espandere le funzionalità di base. Ciascun AVV attribuisce ai componenti nomi differenti, ma tutti comportano lo scambio dei dati personali degli utenti tra il progettista dell'AVV e lo sviluppatore dell'applicazione.

14. Benché la maggior parte degli AVV non condivida il frammento vocale con gli sviluppatori delle applicazioni, questi soggetti trattano comunque dati personali. Inoltre, a seconda della natura della funzionalità fornita, lo sviluppatore delle applicazioni riceve intenzioni e variabili informative che potrebbero includere informazioni sensibili come dati sanitari.

2.2 SOGGETTI OPERANTI NELL'AMBIENTE DELL'AVV

15. Un AVV può coinvolgere numerosi soggetti e intermediari lungo l'intera catena di esecuzione. In pratica si possono individuare fino a cinque soggetti differenti. A seconda dei modelli di business e delle scelte tecnologiche, taluni soggetti possono tuttavia assumere molteplici ruoli, ad esempio progettista e integratore oppure progettista e sviluppatore di applicazioni:

    a. **il fornitore (o il progettista) dell'AVV**: è il soggetto responsabile dello sviluppo dell'AVV, lo progetta e ne definisce le possibilità e le funzionalità predefinite: modalità di attivazione, scelta dell'architettura, accesso ai dati, gestione delle registrazioni, specifiche hardware ecc.;

    b. **lo sviluppatore di applicazioni per l'AVV**: come nel caso delle applicazioni mobili, crea applicazioni che ampliano le funzionalità predefinite dell'AVV; a tal fine è necessario rispettare i limiti di sviluppo imposti dal progettista;

    c. **l'integratore**: è il produttore di oggetti connessi che vuole dotare di un AVV; dovrebbe rispettare i requisiti stabiliti dal progettista;

    d. **il proprietario**: è il responsabile di spazi fisici destinati ad accogliere persone (alloggi, ambienti professionali, veicoli a noleggio ecc.) e intende offrire un AVV ai propri clienti (se possibile con applicazioni dedicate);

    e. **l'utente**: è l'elemento finale della catena di valore dell'AVV e può utilizza-

re tale dispositivo in varie apparecchiature (altoparlanti, televisori, smartphone, orologi ecc.) a seconda del modo e del luogo in cui l'AVV è stato impiegato e configurato.

2.3 DESCRIZIONE DELLE FASI

16. Un AVV può compiere un'azione o accedere a informazioni soltanto se è eseguita una successione di compiti:

    1) dopo essere stato installato in un'apparecchiatura (smartphone, altoparlante, veicolo), l'AVV rimane in attesa. Per la precisione, l'AVV ascolta costantemente, ma finché non viene rilevata una specifica espressione di attivazione, il dispositivo che riceve l'impulso vocale non trasmette nessun audio e non è eseguita nessun'altra operazione se non il rilevamento dell'espressione di attivazione. A tal fine si utilizza una memoria tampone della durata di pochi secondi (si veda la sezione seguente per maggiori dettagli).

    2) L'utente pronuncia l'espressione di attivazione e l'AVV confronta localmente l'audio con l'espressione di attivazione. Se c'è corrispondenza, l'AVV apre un canale d'ascolto e il contenuto audio viene trasmesso immediatamente.

    3) In molti casi, se il trattamento del comando avviene da remoto, dal lato del server si procede a un secondo controllo della pronuncia della parola chiave, per limitare le attivazioni indesiderate.

    4) L'utente formula a voce la propria richiesta, che viene trasmessa direttamente al fornitore dell'AVV. La sequenza del parlato è poi trascritta automaticamente (dal parlato al testo).

    5) Il comando è interpretato mediante tecnologie di trattamento del linguaggio naturale. Si estraggono le intenzioni del messaggio e si individuano le variabili informative (slot). Si ricorre poi a un gestore del dialogo per specificare lo scenario di interazione da implementare con l'utente fornendo lo schema di risposta appropriato.

    6) Se il comando comporta una funzionalità fornita da un'applicazione di terzi (abilità, azione, scorciatoia ecc.), il fornitore dell'AVV trasmette allo sviluppatore dell'applicazione le intenzioni e le variabili informative del messaggio.

    7) Si individua una risposta adattata alla richiesta dell'utente, o una ritenuta tale, laddove la risposta «Non so rispondere alla tua domanda» costituisce una risposta adattata nel caso in cui l'AVV non sia in grado di interpretare correttamente la richiesta. Se necessario si ricorre a risorse remote: banche dati di conoscenze pubblicamente disponibili (enciclopedie online ecc.) o accessibili previa autenticazione (conto bancario, applicazione musicale, conto cliente per gli acquisti online ecc.), mentre le variabili informative sono riempite con le conoscenze recuperate.

    8) Viene creata una frase di risposta e/o individuata un'azione (abbassare le tapparelle, alzare la temperatura, riprodurre un brano musicale, rispondere a una domanda ecc.). La frase è poi sintetizzata (dal testo al parlato) e/o l'azione da eseguire è inviata all'apparecchiatura attivata.

9) L'AVV ritorna in modalità di attesa.

Si fa presente che, benché attualmente il trattamento vocale sia effettuato per la maggior parte su server remoti, alcuni fornitori di AVV stanno sviluppando sistemi che potrebbero eseguire localmente una parte del trattamento[5].

2.4 ESPRESSIONI DI ATTIVAZIONE

17. Per poter essere utilizzato, un AVV dovrebbe essere «attivo». Ciò significa che l'assistente passa a una modalità di ascolto attivo per ricevere ordini e comandi dal proprio utente. Talvolta l'attivazione può essere ottenuta per mezzo di un'azione fisica (ad esempio premendo un pulsante o l'altoparlante intelligente ecc.); tuttavia, quasi tutti gli AVV presenti sul mercato si basano sul rilevamento di un'espressione o una parola di attivazione (detta anche «parola di sveglia/hot word») per passare alla modalità di ascolto attivo.
18. A tal fine l'assistente usa il microfono e alcune capacità informatiche per rilevare se è stata pronunciata la parola chiave. Questa analisi, che è condotta in modo continuativo a partire dal momento in cui l'AVV è acceso, si svolge esclusivamente a livello locale. Le registrazioni audio sono trattate a fini di interpretazione ed esecuzione del comando soltanto dopo che la parola chiave è stata riconosciuta, il che comporta in molti casi l'invio delle registrazioni a server remoti tramite Internet. Il rilevamento della parola chiave si basa sulle tecniche di apprendimento automatico. La principale difficoltà nell'uso di questi metodi è che il rilevamento avviene su base probabilistica. Ciò significa che, per ciascuna parola o espressione pronunciata, il sistema calcola un punteggio di confidenza che indica se la parola chiave è stata effettivamente pronunciata. Se il punteggio è superiore a un valore soglia predefinito, si ritiene che l'evento si sia verificato. È evidente che tale sistema non è esente da errori: in alcuni casi l'attivazione può non essere rilevata anche se la parola chiave è stata pronunciata (falso negativo), mentre in altri l'attivazione può essere rilevata anche se l'utente non ha pronunciato la parola chiave (falso positivo).
19. Nella pratica, si dovrebbe individuare un compromesso accettabile tra questi due tipi di errori per stabilire il valore soglia. Poiché, però, la conseguenza di un falso rilevamento della parola chiave potrebbe essere l'invio di registrazioni audio, è probabile che si verifichino trasmissioni impreviste e indesiderate di dati. Molto spesso i fornitori di AVV che implementano il trattamento remoto usano un meccanismo di rilevamento bifasico: la prima fase è integrata localmente a livello dell'apparecchiatura, mentre la seconda è eseguita su server remoti dove si svolge il successivo trattamento dei dati. In questo caso gli sviluppatori tendono a impostare una soglia relativamente bassa per accrescere l'esperienza dell'utente e garantire che la parola chiave, quando pronunciata, sia riconosciuta quasi sempre (anche se ciò comporta un «eccesso di rilevamento»), per poi effettuare una seconda fase di rilevamento, più restrittiva, sul versante del server.

2.5 FRAMMENTI VOCALI E APPRENDIMENTO AUTOMATICO

20. Poiché si basano su metodi di apprendimento automatico per svolgere una grande varietà di compiti (rilevamento di parole chiave, riconoscimento automatico del parlato, trattamento del linguaggio naturale, sintesi vocale ecc.), gli AVV hanno bisogno di grandi insiemi di dati che devono essere raccolti, selezionati, etichettati ecc.

21. La rappresentazione in eccesso o in difetto di talune caratteristiche statistiche può influenzare lo sviluppo dei compiti basati sull'apprendimento automatico, riflettendosi sui calcoli e, quindi, sulle modalità di funzionamento. Pertanto, non solo la quantità ma anche la qualità dei dati svolge un ruolo importante ai fini della precisione e dell'accuratezza del processo di apprendimento.

22. Per migliorare la qualità dell'AVV e i metodi di apprendimento automatico impiegati, i progettisti di AVV potrebbero voler accedere ai dati relativi all'uso del dispositivo in condizioni reali (ossia a frammenti vocali), allo scopo di migliorarne le prestazioni.

23. Che si tratti di qualificare la banca dati dell'apprendimento o di correggere errori commessi durante l'impiego dell'algoritmo, l'apprendimento e l'addestramento dei sistemi di intelligenza artificiale richiedono necessariamente l'intervento umano. Questa parte del lavoro, detta «lavoro digitale», solleva interrogativi sia sulle condizioni di lavoro che sulla sicurezza. A tale proposito, i mezzi d'informazione hanno segnalato trasferimenti di dati tra progettisti di AVV e subappaltatori che sarebbero avvenuti in assenza delle necessarie garanzie di tutela della vita privata.

3. ELEMENTI DI PROTEZIONE DEI DATI

3.1 QUADRO GIURIDICO

24. Il quadro giuridico dell'UE pertinente per gli AVV è innanzi tutto il RGPD, visto che il trattamento di dati personali è una delle funzioni fondamentali degli AVV. Oltre al RGPD, la direttiva e-privacy[6] stabilisce norme specifiche per tutti i soggetti che intendono archiviare informazioni o accedere a informazioni archiviate nell'apparecchiatura terminale di un abbonato/contraente o un utente nel SEE.

25. Sono conformi alla definizione di «apparecchiatura terminale»[7] gli smartphone, i televisori intelligenti e dispositivi simili dell'Internet degli oggetti. Pur essendo, di per sé, servizi software, gli AVV operano sempre tramite un'apparecchiatura fisica, come un altoparlante intelligente o un televisore intelligente. **Utilizzano le reti di comunicazione elettroniche per accedere a tali dispositivi fisici, che costituiscono un'«apparecchiatura terminale» ai sensi della direttiva e-privacy. Pertanto, le disposizioni dell'articolo 5, paragrafo 3, della direttiva e-privacy si applicano ogniqualvolta l'AVV archivia informazioni o accede a informazioni nell'apparecchiatura fisica cui è collegato[8].**

26. Per poter essere lecita, qualsiasi operazione di trattamento di dati personali successiva alle operazioni di trattamento summenzionate, compreso il trattamento di dati personali ottenuti accedendo a informazioni nell'apparecchiatura terminale, deve avere anche una base giuridica ai sensi dell'articolo 6 del RGPD[9].

27. Poiché il titolare del trattamento, nella richiesta di consenso per l'archiviazione di informazioni o per l'accesso a informazioni a norma dell'articolo 5, paragrafo 3, della direttiva e-privacy, deve informare l'interessato su tutti gli scopi del trattamento (intendendo con ciò il «trattamento successivo»), compreso qualsiasi trattamento che faccia seguito alle operazioni succitate, il consenso di cui all'articolo 6 sarà generalmente la base giuridica più appropriata per il trattamento successivo dei dati personali. È pertanto probabile che il consenso costituisca la base giuridica sia per l'archiviazione di informazioni e l'accesso a informazioni già archiviate, sia per il trattamento dei dati personali successivo alle operazioni di trattamento summenzionate. Di fatto, nel valutare la conformità all'articolo 6 del RGPD si dovrebbe considerare che il trattamento nel suo complesso comporta attività specifiche per le quali il legislatore dell'UE ha cercato di fornire una protezione aggiuntiva[10]. Inoltre, nell'individuare la base legittima appropriata, i titolari del trattamento devono tenere conto dell'impatto sui diritti degli interessati in maniera da rispettare il principio di correttezza[11]. In conclusione, i titolari del trattamento non possono richiamarsi all'articolo 6 del RGPD per abbassare la protezione aggiuntiva di cui all'articolo 5, paragrafo 3, della direttiva e-privacy.

28. Poiché, come indicato nella sezione 2.3 (fasi 2 e 3), gli AVV attuali richiedono l'accesso ai dati vocali archiviati dal dispositivo dell'AVV[12], si applica l'articolo 5, paragrafo 3, della direttiva e-privacy. L'applicabilità dell'articolo 5, paragrafo 3, della direttiva e-privacy significa che l'archiviazione di informazioni e l'accesso a informazioni già archiviate in un AVV richiedono, in linea di principio, il preventivo consenso dell'utente finale[13], ma ammette due eccezioni: primo, se tali operazioni servono per eseguire o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica o, secondo, se sono effettuate nella misura strettamente necessaria per fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente.

29. La seconda eccezione (nella misura strettamente necessaria per fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente) permetterebbe a un fornitore di servizi di AVV di trattare i dati degli utenti per dare esecuzione alle loro richieste (si veda il paragrafo 72 nella sezione 3.4.1) senza il consenso di cui all'articolo 5, paragrafo 3, della direttiva e-privacy. Per contro, **il consenso previsto dall'articolo 5, paragrafo 3, della direttiva e-privacy sarebbe necessario** per l'archiviazione di informazioni o l'accesso a informazioni per **qualsiasi finalità diversa dall'esecuzione delle richieste degli utenti** (ad esempio la profilazione dell'utente). I titolari del trattamento dovrebbero attribuire il consenso a utenti specifici; di conseguenza, dovrebbero trattare i dati degli utenti non registrati soltanto per eseguire le loro richieste.

30. Gli AVV possono captare accidentalmente audio di persone che non intendevano avvalersi di un servizio di AVV. In primo luogo, l'espressione di attivazione può essere modificata in una certa misura e a seconda dell'AVV. Le persone ignare di tale modifica potrebbero usare accidentalmente l'espressione di attivazione aggiornata. In secondo luogo, gli AVV possono captare l'espressione di attivazione per sbaglio o per errore. È altamente improbabile che le due eccezioni previste dall'articolo 5, paragrafo 3, della direttiva e-privacy siano applicabili in caso di attivazione accidentale. Inoltre, il consenso quale definito nel RGPD deve essere «qualsiasi manifestazione di volontà [...] inequivocabile dell'interessato». Pertanto è altamente improbabile che un'attivazione accidentale possa essere considerata un valido consenso. Se un titolare del trattamento si accorge (ad esempio grazie al controllo automatico o umano) che il servizio di AVV ha accidentalmente trattato dati personali, dovrebbe verificare che esista una valida base giuridica per ciascuna finalità del trattamento di tali dati. In caso contrario, i dati raccolti accidentalmente dovrebbero essere cancellati.

31. Va rilevato altresì che i dati personali trattati dagli AVV possono essere di natura altamente sensibile, ad esempio perché comprendono dati personali sia nel contenuto (significato del parlato) sia nelle metainformazioni (sesso o età del parlante ecc.). Il CEPD rammenta che i dati vocali sono dati personali intrinsecamente biometrici[14], motivo per cui, quando sono trattati a fini di identificazione univoca di una persona fisica ovvero sono intrinsecamente dati personali appartenenti a una categoria particolare o sono destinati a esserlo, il trattamento deve avere una valida base giuridica nell'articolo 6 ed essere accompagnato da una deroga all'articolo 9 del RGPD (si veda la sezione 3.7).

3.2 INDIVIDUAZIONE DEL TRATTAMENTO DI DATI E DELLE PARTI INTERESSATE

32. In considerazione delle molteplici possibilità di assistenza che un AVV può fornire in contesti tanto differenti e numerosi della vita quotidiana di un interessato[15], è opportuno rilevare che si dovrebbe prestare particolare attenzione al trattamento dei dati personali, che può essere influenzato del pari da varie parti interessate.

3.2.1 TRATTAMENTO DEI DATI PERSONALI

33. In termini di protezione dei dati personali si possono osservare numerose costanti, indipendentemente dal tipo di AVV che un interessato può usare (ad esempio il tipo di dispositivo, le funzionalità, i servizi o le combinazioni di questi elementi). Tali costanti riguardano la pluralità dei dati personali, degli interessati e del trattamento dei dati in questione.

Pluralità delle categorie di dati personali

34. La definizione di dati personali di cui all'articolo 4, punto 1, del RGPD comprende un'ampia gamma di dati differenti e si applica, in un contesto tec-

nologicamente neutrale, a qualsiasi informazione «riguardante una persona fisica identificata o identificabile»[16]. Qualsiasi interazione di un interessato con un AVV può rientrare nell'ambito di applicazione di questa definizione. Una volta avvenuta l'interazione, durante il funzionamento dell'AVV si possono trattare gruppi differenti di dati personali, come descritto nella sezione 2.4.

35. Dalla richiesta iniziale fino alla risposta, all'azione o al seguito corrispondenti (come l'impostazione di un allarme settimanale), la prima immissione di dati personali genererà pertanto dati personali successivi, tra cui dati primari (ad esempio dati sull'account, registrazioni vocali, cronologia delle richieste), dati osservati (ad esempio dati del dispositivo riguardanti un interessato, registri delle attività, attività online) e dati desunti o derivati (ad esempio profilazione dell'utente). Gli AVV utilizzano il parlato per mediare tra gli utenti e tutti i servizi connessi (ad esempio un motore di ricerca, un negozio online o un servizio di streaming musicale), ma, diversamente da altri intermediari, possono avere pieno accesso al contenuto delle richieste e, quindi, fornire al progettista dell'AVV un'ampia gamma di dati personali, a seconda delle finalità del trattamento.

36. La pluralità dei dati personali trattati quando si utilizza un AVV si riferisce anche a una pluralità di categorie di dati personali cui si dovrebbe prestare attenzione (si veda la sezione 3.7). Il CEPD ricorda che, nel trattamento di categorie particolari di dati[17], l'articolo 9 del RGPD prevede che il titolare del trattamento debba individuare una deroga valida al divieto di trattamento di cui all'articolo 9, paragrafo 1, nonché una base giuridica valida a norma dell'articolo 6, paragrafo 1, per mezzo di strumenti adeguati quali specificati all'articolo 9, paragrafo 2. Il consenso esplicito può essere una deroga valida se il consenso costituisce la base giuridica cui si fa riferimento a norma dell'articolo 6, paragrafo 1. L'articolo 9 rileva altresì (in dettaglio) che gli Stati membri possono introdurre ulteriori condizioni per il trattamento di dati biometrici o di altre categorie particolari di dati.

Pluralità degli interessati

37. Quando si utilizza un AVV, i dati personali sono trattati a partire dalla prima interazione con l'AVV. Per taluni interessati, la prima interazione si riferisce all'acquisto dell'AVV e/o alla configurazione di un account utente (utenti registrati), mentre per altri interessati si riferisce alla prima volta che interagiscono consapevolmente con l'AVV di un altro interessato che ha acquistato e/o configurato tale AVV (utenti non registrati). Oltre a queste due categorie di interessati ce n'è una terza, ossia quella degli utenti accidentali che, siano essi registrati oppure no, fanno inconsapevolmente richieste all'AVV (ad esempio perché pronunciano l'espressione di attivazione corretta senza accorgersi che l'AVV è acceso oppure pronunciano altre parole che l'AVV erroneamente interpreta come l'espressione di attivazione).

38. L'espressione «pluralità degli interessati» si riferisce anche agli utenti multipli di un AVV (ad esempio un dispositivo condiviso tra utenti registrati e non

registrati, tra colleghi, in famiglia, a scuola) e a tipologie di utenti differenziati in base alla loro condizione (ad esempio un adulto, un minore, un anziano o una persona con disabilità). Benché un AVV possa facilitare l'interazione con uno strumento digitale e offrire molti benefici a talune categorie di interessati, è importante considerare le specificità di ciascuna categoria di interessati e il contesto in cui l'AVV è utilizzato.

Pluralità dei trattamenti di dati

39. Anche le tecnologie impiegate per fornire un AVV hanno un impatto sulla quantità dei dati trattati e sui tipi di trattamento. Quanto maggiore è il numero di servizi o caratteristiche offerte dall'AVV e quanto più esso è connesso con altre apparecchiature o servizi gestiti da altri soggetti, tanto maggiori sono la quantità dei dati personali trattati e la ridefinizione delle finalità del trattamento. Ciò si traduce in una pluralità di trattamenti eseguiti da strumenti automatici quali descritti nella sezione 2. Oltre ai mezzi automatici, alcuni trattamenti possono richiedere anche mezzi umani, ad esempio quando la tecnologia implementata comporta l'intervento umano sotto forma di revisione della trascrizione del parlato o di annotazioni sui dati personali che possono essere utilizzate per inserire modelli nuovi in una tecnologia di apprendimento automatico, o ancora quando i dati personali (ad esempio i metadati) sono analizzati da operatori umani per migliorare il servizio fornito da un AVV.

3.2.2 TRATTAMENTO DA PARTE DEI TITOLARI E DEI RESPONSABILI DEL TRATTAMENTO

40. Gli interessati dovrebbero essere in grado di comprendere e individuare i ruoli in questione e di mettersi in contatto o interagire con ciascun soggetto interessato, come prescritto dal RGPD. La distribuzione dei ruoli non dovrebbe andare a discapito degli interessati, per quanto complicati o in evoluzione possano essere gli scenari. Al fine di valutare i rispettivi ruoli, si rinviano i soggetti interessati alle linee guida CEPD 7/2020 in relazione ai concetti di titolare del trattamento e responsabile del trattamento quali definiti dal RGPD[18].

41. Come indicato nel paragrafo 15,i principali operatori nel contesto degli AVV possono essere individuati nei soggetti che svolgono i seguenti ruoli: fornitore o progettista, sviluppatore di applicazioni, integratore, proprietario del dispositivo; ovvero che svolgono una combinazione di questi ruoli. Sono possibili scenari differenti che variano in base alle attività svolte nell'ambito del rapporto professionale tra i soggetti interessati, nonché a seconda della richiesta dell'utente, dei dati personali, delle attività di trattamento dei dati e delle loro finalità. I soggetti/operatori interessati dovrebbero stabilire e comunicare chiaramente agli interessati dal trattamento le condizioni alle quali ciascuno di essi agirà e adempirà ai ruoli risultanti di titolare, contitolare o responsabile del trattamento, come previsto dal RGPD[19]. Ciascun sog-

getto interessato può assumere uno o più ruoli ed essere, quindi, un titolare unico del trattamento, un contitolare del trattamento o un responsabile del trattamento nei riguardi di un determinato trattamento, svolgendo contemporaneamente un ruolo diverso in un diverso trattamento di dati.

42. In termini generali, il progettista può fungere da titolare del trattamento quando definisce le finalità e gli strumenti di un trattamento, ma può agire in qualità di responsabile del trattamento quando tratta dati personali per conto di altri soggetti, come uno sviluppatore di applicazioni. In tali casi l'utente dell'AVV sarebbe pertanto soggetto a più titolari del trattamento: lo sviluppatore di applicazioni e il progettista. È altresì possibile che il progettista, l'integratore e lo sviluppatore siano raggruppati in un'unica entità operante come titolare unico del trattamento. Comunque sia, le qualifiche applicabili devono essere stabilite sulla base di un'analisi caso per caso.

Esempio 1

il progettista dell'AVV tratta i dati dell'utente per molte finalità, comprese quelle di migliorare le abilità di comprensione vocale dell'AVV e di rispondere accuratamente alle richieste. Per tale motivo e benché questa finalità possa comportare il trattamento di dati risultanti dall'uso di applicazioni fornite da terzi, esiste un solo titolare del trattamento: il progettista dell'AVV per conto e per le finalità del quale viene eseguito il trattamento.

Esempio 2

una banca offre ai propri clienti un'applicazione che può essere interrogata direttamente tramite l'AVV per gestire i loro conti.

Nel trattamento dei dati personali sono coinvolti due soggetti: il progettista dell'AVV e lo sviluppatore dell'applicazione bancaria.

Nello scenario prospettato, la banca è il titolare del trattamento per la fornitura del servizio, essendo il soggetto che stabilisce le finalità e i mezzi essenziali del trattamento correlato all'applicazione che consente l'interazione con l'assistente. Infatti, la banca mette a disposizione un'applicazione dedicata che consente all'utente – un suo cliente – di gestire i propri conti da remoto. Inoltre, la banca stabilisce i mezzi di trattamento scegliendo un idoneo responsabile del trattamento, che è il progettista dell'AVV e può svolgere un importante ruolo di assistenza grazie alla propria competenza nella definizione di questi mezzi (ad esempio, può gestire la piattaforma di sviluppo che consente l'integrazione delle applicazioni di terzi nell'AVV e, pertanto, fissa il quadro e le condizioni che gli sviluppatori delle applicazioni devono rispettare).

43. Dal punto di vista dell'interessato, vale la pena rilevare che i medesimi dati personali possono essere trattati da una pluralità di soggetti, anche se l'interessato non si aspetta in realtà che altri soggetti, diversi dal fornitore dell'AVV, siano coinvolti nella catena di trattamento. Pertanto, quando un interessato interagisce con il fornitore dell'AVV in riferimento ai propri dati personali (ad esempio per l'esercizio dei propri diritti di interessato), tale azione non vale automaticamente anche per gli stessi dati personali che sono trattati da un altro soggetto interessato. Se questi soggetti sono titolari del trattamento indipendenti, è importante che gli interessati ricevano un'informativa chiara contenente l'indicazione delle varie fasi e dei diversi operatori del trattamento. Inoltre, nel caso di contitolari del trattamento va chiarito se ciascuno di essi è competente per il rispetto di tutti i diritti dell'interessato, oppure quale contitolare è competente per quale diritto[20].

Esempio 3

in questo scenario il progettista dell'AVV vuole utilizzare i dati raccolti e trattati ai fini del servizio erogato dalla banca per migliorare il sistema di riconoscimento vocale dell'AVV. Pertanto, il progettista dell'AVV che tratta i dati per finalità proprie avrà lo status di titolare del trattamento per questa specifica attività di trattamento.

44. Poiché nella catena del trattamento possono essere coinvolti molti soggetti, e anche molto personale, in assenza di misure e garanzie appropriate potrebbero verificarsi situazioni di rischio. I titolari del trattamento sono responsabili dell'adozione di tali misure e pertanto dovrebbero concentrarsi sulla protezione dei dati personali, in particolare scegliendo partner professionali e responsabili del trattamento idonei, applicando la tutela della vita privata come impostazione predefinita[21], implementando adeguati strumenti di sicurezza e altri strumenti previsti dal RGPD, quali audit e accordi legali (ad esempio l'articolo 26 per i contitolari o l'articolo 28 per i responsabili del trattamento).
45. L'ambiente dell'AVV è complesso perché un numero potenzialmente elevato di soggetti potrebbe scambiare e trattare dati personali in qualità di titolari o responsabili del trattamento. È della massima importanza chiarire il ruolo di ciascun soggetto rispetto a ciascun trattamento, nonché attenersi al principio della minimizzazione dei dati anche in relazione allo scambio di dati.
46. Inoltre, i titolari del trattamento dovrebbero vigilare sui trasferimenti di dati personali e garantire il livello di protezione richiesto durante tutta la catena del trattamento, in particolare quando utilizzano dispositivi collocati al di fuori del SEE.

3.3 TRASPARENZA

47. Poiché trattano dati personali (ad esempio la voce degli utenti, il luogo o il contenuto della comunicazione), gli AVV devono essere conformi ai requisiti in materia di trasparenza di cui al RGPD, come disciplinati dall'articolo 5, paragrafo 1, lettera a), e dagli articoli 12 e 13 (specificati nel considerando 58). I titolari del trattamento sono tenuti a comunicare agli utenti il trattamento dei loro dati personali in forma concisa, trasparente e intelligibile, nonché in un modo facilmente accessibile.

48. La mancata comunicazione delle informazioni necessarie costituisce una violazione degli obblighi che può incidere sulla liceità del trattamento dei dati. È obbligatorio conformarsi al requisito della trasparenza in quanto esso funge da meccanismo di controllo del trattamento dei dati e consente agli utenti di esercitare i propri diritti. Se gli utenti sono adeguatamente informati delle modalità di utilizzo dei loro dati, per i titolari del trattamento sarà più difficile usare scorrettamente gli AVV per finalità che vanno ben oltre le aspettative degli utenti. Ad esempio, tecnologie brevettate mirano a dedurre lo stato di salute e le condizioni emotive dalla voce dell'utente adattando di conseguenza i servizi forniti.

49. Conformarsi ai requisiti di trasparenza può essere particolarmente difficile per il fornitore di servizi di AVV o per qualsiasi altro soggetto che opera in quanto titolare del trattamento. In considerazione della natura specifica degli AVV, i titolari del trattamento devono superare numerosi ostacoli per conformarsi ai requisiti di trasparenza previsti dal RGPD:

- **utenti multipli**: i titolari del trattamento dovrebbero informare tutti gli utenti (registrati, non registrati, accidentali), non soltanto l'utente che ha installato l'AVV;
- **complessità dell'ambiente**: come spiegato nella sezione sul contesto tecnologico, le identità e i ruoli dei soggetti che trattano dati personali in rapporto all'utilizzo di un AVV sono tutt'altro che evidenti per gli utenti;
- **specificità dell'interfaccia vocale**: i sistemi digitali non sono ancora pronti per interazioni esclusivamente vocali, come dimostra l'uso quasi sistematico di schermi complementari. Nondimeno è necessario adattarsi all'interfaccia vocale ed essere in grado di informare l'utente in modo chiaro e corretto mediante tale interfaccia.

50. Gli AVV possono essere considerati apparecchiature a stati finiti che passano attraverso una serie di stati nel corso del funzionamento ordinario. Possono ascoltare localmente per il rilevamento di espressioni di attivazione o interagire con un server remoto per eseguire un comando; possono però assumere anche molti altri stati a seconda del contesto (ad esempio se c'è un rumore ambientale di fondo) o se l'utente parla con loro (ad esempio possono interloquire con un utente identificato o sconosciuto). Purtroppo, queste situazioni si verificano nel contesto di una sostanziale asimmetria informativa rispetto all'utente, che molto raramente sa se il dispositivo stia ascoltando e ancor meno in quale stato esso si trovi.

51. Si raccomanda vivamente ai progettisti di AVV e agli sviluppatori di adottare misure adeguate per ovviare a tali asimmetrie, rendendo più interattivo il funzionamento degli AVV. Gli utenti dovrebbero essere informati dello stato in cui si trova il dispositivo in un dato momento. Questa maggiore trasparenza si può ottenere rendendo più interattivo il dialogo uomo-macchina (ad esempio, il dispositivo potrebbe confermare, in qualche modo, il ricevimento di un comando vocale) oppure inviando segnali specifici per comunicare lo stato del dispositivo. A tal fine si possono prendere in considerazione molte opzioni, che vanno dall'uso di specifiche conferme vocali e icone o segnali luminosi visibili fino all'utilizzo di schermi sul dispositivo.

52. Questi aspetti sono particolarmente rilevanti se si tiene conto della pluralità degli utenti e della presenza, tra loro, di categorie vulnerabili come minori, anziani o utenti con disabilità audio-visive.

53. Dalle tematiche sopra esaminate emergono due interrogativi importanti: qual è il modo più praticabile per informare gli utenti e qual è il momento più adatto per informarli? Tali questioni dovrebbero essere ulteriormente approfondite in due situazioni differenti, a seconda che l'AVV abbia un solo utente (ad esempio uno smartphone personale) o potenzialmente utenti multipli (ad esempio un dispositivo domotico). Quando si utilizza una tecnologia AVV, potrebbe verificarsi anche un'inversione di queste due configurazioni di base poiché, ad esempio, un utente potrebbe collegare il proprio smartphone personale con l'automobile. L'AVV dello smartphone, che si potrebbe ragionevolmente supporre sia utilizzato soltanto dall'utente in questione, è ora «esteso» agli altri dispositivi presenti nell'automobile.

54. Attualmente gli AVV sono connessi a un account utente e/o sono configurati da un'applicazione che richiede l'esistenza di un account utente. Le modalità con cui i titolari del trattamento potrebbero informare gli utenti sulla propria politica per la privacy durante la configurazione dell'AVV dovrebbero essere definite in conformità delle linee guida del gruppo di lavoro Articolo 29 in materia di trasparenza. Le applicazioni dovrebbero mettere a disposizione le informazioni necessarie in un negozio online prima dello scaricamento[22]. In tal modo le informazioni sarebbero fornite alla prima occasione possibile e anche in ultima istanza, ossia quando si ottengono i dati personali. Alcuni fornitori di AVV includono applicazioni di terzi nelle impostazioni predefinite dei propri dispositivi affinché queste applicazioni possano eseguire le altre per mezzo di specifiche espressioni di attivazione. Gli AVV che adottano questa strategia basata sull'uso di applicazioni di terzi dovrebbero accertarsi che gli utenti ricevano anche le informazioni necessarie sul trattamento da parte di terzi.

55. Tuttavia, molti progettisti di AVV richiedono account utenti per collegare il servizio dell'AVV con una pluralità di altri servizi come la posta elettronica, lo streaming di video o gli acquisti, per citarne solo alcuni. La decisione del progettista di AVV di collegare l'account con molti servizi diversi richiede informative sulla privacy molto lunghe e complesse. La lunghezza e la complessità di tali informative ostacolano notevolmente il rispetto del principio di trasparenza.

Esempio 4

un progettista di AVV richiede agli utenti il possesso di un account per poter accedere al servizio di AVV. Questo account utente non è specifico del servizio di AVV e può essere utilizzato anche per altri servizi offerti dal progettista di AVV, come la posta elettronica, l'archiviazione sul cloud e i media sociali. Per creare l'account gli utenti devono leggere e accettare un'informativa sulla privacy di 30 pagine, contenente informazioni sul trattamento dei dati personali da parte di tutti i servizi che potrebbero essere collegati con l'account.
Le informazioni fornite dal progettista dell'AVV in questo caso non possono essere considerate concise; inoltre, la loro complessità riduce la trasparenza richiesta. Pertanto il progettista di AVV non sarebbe conforme ai requisiti in materia di trasparenza di cui agli articoli 12 e 13 del RGPD.

56. Benché il modo più comune per comunicare le informazioni necessarie sia la forma scritta, il RGPD consente «altri mezzi». Il considerando 58 prevede esplicitamente che le informazioni potrebbero essere fornite in formato elettronico, ad esempio attraverso un sito web. Inoltre, nella scelta del metodo appropriato per informare gli interessati si dovrebbe tenere conto delle circostanze specifiche, come le modalità in cui il titolare del trattamento e l'interessato interagiscono altrimenti tra loro[23]. Un'opzione per i dispositivi privi di schermo potrebbe consistere nel fornire un link di facile comprensione, direttamente o tramite la posta elettronica. Per comunicare le informazioni necessarie si potrebbe ricorrere a soluzioni già esistenti, come le prassi dei call centre di comunicare al chiamante che la sua telefonata viene registrata e di rinviarlo alle proprie informative sulla privacy. I limiti posti dalla mancanza di schermo in taluni AVV non esonerano il titolare del trattamento dall'obbligo di fornire le informazioni necessarie ai sensi del RGPD quando configura l'AVV ovvero installa o utilizza un'applicazione di AVV. I fornitori di AVV e gli sviluppatori dovrebbero elaborare interfacce basate sulla voce per facilitare la comunicazione delle informazioni obbligatorie.
57. Gli AVV potrebbero essere molto utili per gli utenti con disabilità visive, in quanto offrono possibilità di interazione alternative rispetto ai servizi informatici tradizionalmente basati su informazioni visive. A norma dell'articolo 12, paragrafo 1, del RGPD le informazioni necessarie possono essere fornite oralmente soltanto su richiesta dell'interessato, non come approccio predefinito. Tuttavia, i limiti degli AVV privi di schermo richiederebbero l'uso di strumenti automatici di informazione orale, che potrebbero essere potenziati con mezzi scritti. Quando si ricorre all'audio per informare gli interessati, i titolari del trattamento dovrebbero fornire le informazioni necessarie in modo chiaro e conciso. Inoltre, gli interessati dovrebbero poter riascoltare le comunicazioni[24].
58. Adottare le misure appropriate per conformarsi ai requisiti di trasparenza previsti dal RGPD è più complesso quando l'AVV ha utenti multipli diversi dal proprietario del dispositivo. I progettisti di AVV devono valutare come

informare correttamente gli utenti non registrati e accidentali quando sono trattati i loro dati personali. Se il consenso costituisce la base giuridica del trattamento dei dati dell'utente, esso è valido soltanto se l'utente è stato informato correttamente[25].

59. Per conformarsi al RGPD i titolari del trattamento dovrebbero trovare un modo per informare non soltanto gli utenti registrati, ma anche quelli non registrati e gli utenti accidentali degli AVV. Questi utenti dovrebbero essere informati alla prima occasione possibile **e in ultima istanza, cioè al momento del** trattamento. L'adempimento pratico di tale condizione potrebbe risultare particolarmente difficile.

60. Inoltre, talune specificità aziendali non dovrebbero nuocere agli interessati. Considerato che molti soggetti/operatori interessati sono società multinazionali o sono ben noti in specifici ambiti di attività (ad esempio telecomunicazioni, commercio elettronico, tecnologie dell'informazione, attività web), dovrebbe essere chiaro in quale modo essi forniscono un servizio di AVV. La comunicazione di informazioni adeguate dovrebbe far comprendere agli interessati se il loro utilizzo dell'AVV comporterà collegamenti con altre attività di trattamento gestite dal fornitore di servizi di AVV (ad esempio telecomunicazioni, commercio elettronico, tecnologie dell'informazione o attività web) che esulano dall'uso in senso stretto dell'AVV.

Esempio 5

un progettista di AVV che offre anche una piattaforma per media sociali e un motore di ricerca richiede all'utente di collegare il proprio account con l'assistente per poterlo utilizzare. Il collegamento tra l'account dell'utente e l'AVV permette quindi al progettista di migliorare il profilo dei propri utenti grazie all'uso dell'assistente, delle applicazioni (o delle abilità) installate, degli ordini fatti ecc. Pertanto, le interazioni con l'assistente rappresentano una nuova fonte di informazioni collegata a un utente. Il progettista dell'AVV dovrebbe fornire agli utenti informazioni chiare sulle modalità di trattamento dei loro dati per ciascun servizio nonché strumenti di controllo per autorizzare o meno l'uso dei dati a fini di profilazione.

Raccomandazioni

61. Se gli utenti sono informati del trattamento dei dati personali da parte dell'AVV per mezzo di un'informativa sulla privacy di un account utente e tale account è collegato ad altri servizi indipendenti (ad esempio posta elettronica o acquisti online), il CEPD raccomanda che detta informativa comprenda una sezione nettamente distinta concernente il trattamento dei dati personali da parte dell'AVV.

62. Le informazioni fornite all'utente dovrebbero corrispondere esattamente alla raccolta e al trattamento effettuati. Anche se un campione vocale contiene alcune metainformazioni (ad esempio il livello di stress del parlante), non

è automaticamente chiaro se venga eseguita la relativa analisi. È essenziale che i titolari del trattamento comunichino con trasparenza quali aspetti specifici dei dati grezzi trattano.

63. Inoltre, dovrebbe essere evidente in ogni momento in quale stato si trova l'AVV. Gli utenti dovrebbero poter accertare se un AVV stia ascoltando sul proprio circuito chiuso e, in particolare, se stia trasmettendo informazioni al proprio back-end. Questa informazione dovrebbe essere accessibile anche alle persone con disabilità quali il daltonismo (discromatopsia) e la sordità (anacusia). Occorre considerare in particolare che gli AVV suggeriscono uno scenario d'uso in cui non è necessario il contatto visivo con il dispositivo. Pertanto, tutti i feedback degli utenti, incluse le variazioni di stato, dovrebbero essere disponibili quanto meno in formato sia visivo che acustico.

64. Particolare attenzione è richiesta altresì nel caso dei dispositivi che consentono di aggiungere funzionalità di terzi (applicazioni per AVV). Benché talune informazioni di carattere generale possano essere fornite agli utenti quando sono loro ad aggiungere tale funzionalità (per decisione propria), nell'uso normale del dispositivo i confini tra i vari titolari del trattamento coinvolti possono essere molto meno netti, nel senso che gli utenti potrebbero non essere sufficientemente informati su come e da chi (e in quale misura) siano trattati i loro dati in una specifica interrogazione.

65. Tutte le informazioni relative a trattamenti basati su dati raccolti e ricavati attraverso l'elaborazione di registrazioni vocali dovrebbero essere anch'esse a disposizione degli utenti in conformità dell'articolo 12 del RGPD.

66. I titolari del trattamento dell'AVV dovrebbero comunicare in maniera trasparente quale tipo di informazioni un AVV può ricavare in merito all'ambiente circostante, come, ad esempio, la presenza di altre persone nella stanza, la musica in sottofondo, eventuali trattamenti della voce per fini medici, commerciali o d'altro genere, la presenza di animali da compagnia ecc.

3.4 LIMITAZIONE DELLA FINALITÀ E BASE GIURIDICA

67. Il trattamento di richieste vocali da parte degli AVV ha una finalità evidente: l'esecuzione della richiesta. Tuttavia, ci sono spesso finalità aggiuntive che non sono altrettanto evidenti, come il miglioramento delle capacità dell'AVV di comprendere il linguaggio naturale mediante il modello di addestramento dell'AVV con tecniche di apprendimento automatico. Tra le finalità più comuni del trattamento di dati personali da parte degli AVV figurano:

- l'esecuzione delle richieste degli utenti;
- il miglioramento dell'AVV mediante addestramento del modello di apprendimento automatico e revisione umana, nonché l'etichettatura delle trascrizioni del parlato;
- l'identificazione dell'utente (con dati vocali);
- la profilazione dell'utente a fini di personalizzazione dei contenuti o della pubblicità.

68. A causa del loro ruolo di intermediari e delle caratteristiche di progettazione, gli AVV trattano un'ampia varietà di dati personali e non personali. Per tale motivo è possibile che i dati personali siano trattati per molte finalità che esulano dall'esecuzione delle richieste degli utenti e che potrebbero restare totalmente ignote. Analizzando i dati raccolti tramite gli AVV si possono conoscere o dedurre gli interessi, gli orari, i percorsi di guida o le abitudini dell'utente. Ciò renderebbe possibile il trattamento di dati personali per fini non previsti [ad esempio per l'analisi del sentiment o la valutazione dello stato di salute[26]], circostanza che andrebbe ben al di là delle ragionevoli aspettative degli utenti.

69. I titolari del trattamento dovrebbero specificare chiaramente la o le proprie finalità in riferimento al contesto d'uso dell'AVV, in modo tale che esse siano comprese chiaramente dagli interessati (ad esempio presentando le finalità suddivise per categorie). A norma dell'articolo 5, paragrafo 1, del RGPD i dati personali dovrebbero essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità.

3.4.1 ESECUZIONE DELLE RICHIESTE DEGLI UTENTI

70. Un AVV serve principalmente all'emissione di comandi vocali che devono essere eseguiti dall'AVV o da un'applicazione o un servizio ad esso associati (ad esempio un servizio di streaming musicale, un servizio di mappatura o un dispositivo di blocco elettronico). Pertanto, la voce dell'utente e, potenzialmente, altri dati (ad esempio la posizione dell'utente quando chiede l'indicazione del percorso per raggiungere una determinata destinazione) potrebbero essere oggetto di trattamento.

> Esempio 6
>
> il passeggero di un'automobile intelligente dotata di un AVV chiede che gli sia indicato il percorso verso il distributore più vicino. L'AVV tratta la voce dell'utente per comprendere il comando e la posizione dell'automobile per trovare il percorso, che poi trasmette alla componente intelligente affinché lo visualizzi sullo schermo dell'automobile.

71. Nella misura in cui il trattamento dei comandi vocali comporta l'archiviazione di informazioni o l'accesso a informazioni già archiviate nelle apparecchiature terminali dell'utente finale, va rispettato l'articolo 5, paragrafo 3, della direttiva e-privacy. L'articolo 5, paragrafo 3, non soltanto stabilisce il principio generale secondo cui l'archiviazione o l'accesso richiedono il preventivo consenso dell'utente finale, bensì prevede anche una deroga a tale principio del consenso «nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio». Se dunque la voce è trattata al fine di dare esecuzione alle richieste degli utenti, a tale trattamento non si

applica il requisito del consenso preventivo.

72. Come già indicato, per essere lecita, qualsiasi operazione di trattamento di dati personali successiva all'archiviazione di informazioni o all'accesso a informazioni archiviate nell'apparecchiatura terminale degli utenti finali deve avere una base giuridica a norma dell'articolo 6 del RGPD.

73. Nell'AVV avvengono due operazioni di trattamento consecutive. Come osservato sopra, la prima di esse richiede l'accesso all'AVV (per cui devono essere soddisfatte le condizioni dell'articolo 5, paragrafo 3, della direttiva e-privacy). Oltre all'adempimento di queste condizioni, la seconda operazione richiede anche l'esistenza di una base giuridica a norma dell'articolo 6 del RGPD.

74. Quando si decide di utilizzare un AVV, l'utente iniziale deve di norma creare un account per attivare l'AVV. In altri termini, questa situazione fa riferimento a un rapporto contrattuale[27] tra l'utente registrato e il titolare del trattamento dell'AVV. In considerazione del suo obiettivo sostanziale e fondamentale, la finalità principale di tale contratto è quella di utilizzare l'AVV per dare esecuzione alla richiesta di assistenza dell'utente.

75. Qualsiasi trattamento di dati personali che sia necessario per eseguire la richiesta di un utente può dunque essere ricondotto all'esecuzione del contratto quale base giuridica[28]. Questo trattamento comprende, in particolare, la captazione della richiesta vocale dell'utente, la sua trascrizione e interpretazione, le informazioni scambiate con fonti di conoscenze per preparare la risposta e, successivamente, la trasformazione in una risposta vocale finale che conclude la richiesta dell'utente.

76. L'esecuzione di un contratto può costituire una base giuridica per il trattamento di dati personali mediante l'apprendimento automatico se ciò è necessario per l'erogazione del servizio. Il trattamento di dati personali mediante l'apprendimento automatico per altre finalità non necessarie, come il miglioramento del servizio, non dovrebbe essere ricondotto a quella base giuridica.

77. Infine, ma non meno importante, non si dovrebbero confondere le due diverse basi giuridiche dell'esecuzione del contratto e del consenso di cui al RGPD. Il consenso fornito ai fini della stipula di un contratto, ossia ai fini dell'accettazione del vincolo contrattuale, costituisce condizione per la validità del contratto in questione e non ha alcun rapporto con lo specifico significato del consenso di cui al RGPD[29].

78. Qualora l'utilizzo di un AVV non richieda la preventiva configurazione di un account utente per l'AVV stesso, il consenso potrebbe costituire una possibile base giuridica.

3.4.2 MIGLIORAMENTO DELL'AVV MEDIANTE ADDESTRAMENTO DEI SISTEMI DI APPRENDIMENTO AUTOMATICO E REVISIONE MANUALE DEL PARLATO E DELLE TRASCRIZIONI

79. Gli accenti e le variazioni dell'eloquio umano sono numerosi. Benché gli AVV siano immediatamente operativi, è possibile migliorare le loro prestazioni

adattandoli alle caratteristiche specifiche del modo di parlare dell'utente. Come menzionato nella sezione 2.6, questo processo di adattamento si fonda su metodi di apprendimento automatico e consta di due fasi: l'inclusione, nella serie di dati per l'addestramento dell'AVV, di dati nuovi raccolti presso gli utenti e la revisione umana dei dati trattati per l'esecuzione di una parte delle richieste.

Esempio 7

l'utente di un AVV deve pronunciare tre volte lo stesso comando vocale perché l'AVV non lo capisce. I tre comandi vocali e le relative trascrizioni sono trasmessi a revisori umani affinché controllino e correggano le trascrizioni. I comandi vocali e le trascrizioni riviste vengono aggiunti alla serie di dati per addestrare l'AVV e quindi migliorarne le prestazioni.

80. Le attività di trattamento descritte nell'esempio non dovrebbero essere considerate (strettamente) necessarie «all'esecuzione di un contratto» ai sensi dell'articolo 6, paragrafo 1, lettera b), del RGPD, e richiedono pertanto una base giuridica diversa da quella prevista dall'articolo 6 di tale regolamento. Ciò principalmente perché gli AVV sono immediatamente operativi e possono da subito svolgere tutte le operazioni (strettamente) necessarie all'esecuzione del contratto. Il comitato europeo per la protezione dei dati non ritiene che l'articolo 6, paragrafo 1, lettera b), costituisca in via generale un'idonea base giuridica per un trattamento finalizzato al miglioramento di un servizio o allo sviluppo di nuove funzioni nel contesto di un servizio esistente. Nella maggior parte dei casi, un utente stipula un contratto per avvalersi di un servizio esistente. Benché la possibilità di apportare miglioramenti e modifiche a un servizio possa essere sistematicamente inclusa nelle clausole contrattuali, tale trattamento non può di norma essere considerato oggettivamente necessario all'esecuzione del contratto stipulato con l'utente.

3.4.3 IDENTIFICAZIONE DELL'UTENTE[30] (CON DATI VOCALI)

81. L'uso di dati vocali a fini di identificazione dell'utente implica il trattamento di dati biometrici quali definiti nell'articolo 4, punto 14, del RGPD. Pertanto, il titolare del trattamento dovrà individuare una deroga a norma dell'articolo 9 del RGPD, in aggiunta all'individuazione di una base giuridica ai sensi dell'articolo 6 di tale regolamento[31].
82. Tra le deroghe elencate nell'articolo 9 del RGPD, soltanto il consenso esplicito degli interessati sembra applicabile a questa finalità specifica.
83. Tuttavia, poiché questa finalità richiede l'applicazione del regime giuridico specifico di cui all'articolo 9 del RGPD, nella sezione 3.8 sono riportati ulteriori dettagli relativi al trattamento di categorie particolari di dati.

3.4.4 PROFILAZIONE DELL'UTENTE A FINI DI PERSONALIZZAZIONE DEI CONTENUTI O DELLA PUBBLICITÀ

84. Come indicato sopra, gli AVV hanno accesso al contenuto di tutti i comandi vocali anche quando sono impostati per i servizi erogati da terzi. Grazie a questo accesso, il progettista di AVV sarebbe in grado di definire profili dell'utente molto accurati che potrebbero essere usati per offrire servizi o messaggi pubblicitari personalizzati.

> Esempio 8
>
> ogni volta che l'utente di un AVV effettua una ricerca in Internet, l'AVV aggiunge etichette che segnalano gli argomenti d'interesse per il profilo dell'utente. I risultati di ogni nuova ricerca sono presentati all'utente secondo un ordine basato su tali etichette.
>
> Esempio 9
>
> ogni volta che l'utente di un AVV effettua un acquisto presso un servizio di commercio elettronico, l'AVV archivia una registrazione dell'ordine di acquisto. Il fornitore di AVV permette a terzi di inviare all'utente dell'AVV avvisi pubblicitari mirati basati sugli acquisti pregressi.

85. La personalizzazione dei contenuti può costituire un elemento intrinseco e previsto di un AVV (ma non è sempre così). Se tale trattamento possa essere considerato intrinseco al servizio fornito dall'AVV dipende dall'esatta natura del servizio prestato, dalle aspettative di un interessato medio (fondate non soltanto sulle condizioni del servizio, ma anche sul modo in cui questo viene promosso nei confronti degli utenti), nonché dalla possibilità o meno che il servizio sia prestato senza personalizzazione[32].

86. Se la personalizzazione avviene nel contesto di un rapporto contrattuale e in quanto parte di un servizio esplicitamente richiesto dall'utente finale (e se il trattamento è limitato a quanto strettamente necessario all'erogazione del servizio), il trattamento può essere basato sull'articolo 6, paragrafo 1, lettera b), del RGPD.

87. Se il trattamento non è strettamente «necessario all'esecuzione di un contratto» ai sensi dell'articolo 6, paragrafo 1, lettera b), del RGPD, il fornitore di AVV deve chiedere, in linea di principio, il consenso dell'interessato. Infatti, poiché il consenso sarà richiesto a norma dell'articolo 5, paragrafo 3, della direttiva e-privacy per l'archiviazione di informazioni o l'accesso a informazioni archiviate (si vedano sopra i paragrafi 28-29), anche il consenso di cui all'articolo 6, paragrafo 1, lettera a), del RGPD costituirà, in linea di principio, la base giuridica appropriata per il trattamento dei dati personali successivo a queste operazioni, visto che in taluni casi il riferimento al legittimo interesse potrebbe rischiare di compromettere l'ulteriore livello di protezione previsto dall'articolo 5, paragrafo 3, della direttiva e-privacy.

88. Per quanto riguarda la profilazione dell'utente a fini pubblicitari, va rilevato che questa finalità non è mai considerata un servizio esplicitamente richiesto dall'utente finale. Pertanto, in caso di trattamento svolto a questo fine il consenso degli utenti dovrebbe essere raccolto sistematicamente.

Raccomandazioni

89. Gli utenti dovrebbero essere informati della finalità del trattamento dei dati personali e tale finalità dovrebbe corrispondere alle loro aspettative in merito all'apparecchiatura acquistata. Se l'apparecchiatura è un AVV, la finalità (dal punto di vista dell'utente) consiste evidentemente nel trattamento della voce dell'utente al solo fine di interpretare la sua richiesta e fornire risposte adeguate (che si tratti di risposte a interrogazioni o di altre reazioni come il controllo remoto di un interruttore della luce).
90. Nel caso in cui il trattamento dei dati personali sia fondato sul consenso, «il consenso dell'interessato deve essere espresso in relazione a "una o più specifiche" finalità e [...] l'interessato deve poter scegliere in relazione a ciascuna di esse». Inoltre, «il titolare del trattamento che richiede il consenso per finalità diverse dovrebbe prevedere una possibilità di adesione distinta per ciascuna finalità, in modo da permettere all'utente di esprimere un consenso specifico per le finalità specifiche»[33]. Ad esempio, gli utenti dovrebbero avere la possibilità di acconsentire o non acconsentire separatamente alla revisione e all'etichettatura manuali delle trascrizioni del parlato o all'uso dei propri dati vocali a fini di identificazione/autenticazione (si veda la sezione 3.7).

3.5 TRATTAMENTO DEI DATI RELATIVI A MINORI

91. Anche i minori possono interagire con gli AVV o creare profili propri connessi con quelli degli adulti. Alcuni AVV sono integrati in apparecchiature specificamente destinate ai minori.
92. Se la base giuridica del trattamento è l'esecuzione di un contratto, le condizioni per il trattamento dei dati relativi a minori dipendono dal diritto contrattuale nazionale.
93. Se la base giuridica del trattamento è il consenso a norma dell'articolo 8, paragrafo 1, del RGPD, il trattamento dei dati del minore è lecito soltanto «ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.». Ne consegue che, ai fini della conformità al RGPD, nei casi in cui la base giuridica è il consenso, occorre richiedere l'esplicito permesso dei genitori o dei tutori del minore per poter raccogliere, trattare e archiviare i dati del minore (voce, trascrizioni ecc.).
94. I controlli parentali sono disponibili in una certa misura, ma nella loro forma attuale non sono di facile utilizzo (ad esempio è necessario iscriversi a un

nuovo servizio) o hanno capacità limitate. I titolari del trattamento dovrebbero investire nello sviluppo di strumenti che consentano ai genitori o ai tutori di controllare l'uso degli AVV da parte dei minori.

3.6 CONSERVAZIONE DEI DATI

95. Gli AVV trattano e generano un'ampia varietà di dati personali come la voce, le trascrizioni del parlato, i metadati o i log di sistema. Questi dati potrebbero essere trattati per un'ampia gamma di finalità quali l'erogazione di un servizio, il miglioramento del trattamento del linguaggio naturale, la personalizzazione o la ricerca scientifica. In linea con il principio di limitazione della conservazione previsto dal RGPD, gli AVV dovrebbero conservare i dati soltanto per il tempo necessario a conseguire le finalità per cui i dati personali sono trattati. Pertanto, i periodi di conservazione dei dati dovrebbero dipendere dalle differenti finalità del trattamento. I fornitori di servizi AVV o i terzi che forniscono servizi tramite gli AVV dovrebbero valutare quale debba essere il periodo massimo di conservazione per ciascuna serie di dati e ciascuna finalità.

96. Al principio di limitazione della conservazione dei dati è strettamente collegato il principio di minimizzazione dei dati. I titolari del trattamento devono, infatti, limitare non soltanto il periodo di conservazione dei dati, ma anche la loro tipologia e quantità.

97. Essi dovrebbero porsi, tra gli altri, i seguenti interrogativi: è necessario archiviare tutte le registrazioni vocali o tutte le trascrizioni per conseguire la finalità X? È necessario conservare i dati vocali dopo che è stata archiviata la trascrizione? Se sì, per quale finalità? Per quanto tempo i dati vocali o quelli trascritti sono necessari a ciascuna finalità? Dalla risposta a questi e simili interrogativi dipenderanno i periodi di conservazione che dovrebbero far parte delle informazioni disponibili agli interessati.

98. Alcuni AVV archiviano per impostazione predefinita dati personali, quali frammenti di voce o trascrizioni, per un periodo indefinito e forniscono nel contempo agli utenti i mezzi per cancellare tali dati. Conservare i dati personali per un periodo indefinito è in contrasto con il principio di limitazione della conservazione. Fornire agli utenti mezzi per cancellare i propri dati personali non esonera i titolari del trattamento dalla responsabilità di definire e applicare una politica per la conservazione dei dati.

99. La progettazione degli AVV deve tenere conto dei controlli degli utenti finalizzati a consentire la cancellazione dei loro dati personali nelle rispettive apparecchiature e in tutti i sistemi di archiviazione remoti. La presenza di questi controlli può essere necessaria per soddisfare varie tipologie di richieste degli utenti, ad esempio una richiesta di cancellazione o la revoca di un consenso precedentemente accordato. La progettazione di alcuni AVV non ha tenuto conto di questo requisito[34].

100. Come in altri contesti, i titolari del trattamento possono avere la necessità

di conservare dati personali come prova dell'erogazione di un servizio a un utente, in adempimento di un obbligo giuridico. I titolari del trattamento possono conservare dati personali su questo fondamento; tuttavia, i dati conservati dovrebbero essere quelli minimi necessari all'adempimento dell'obbligo giuridico ed essere conservati per il periodo minimo possibile. Ovviamente i dati conservati a fini di adempimento di un obbligo giuridico non dovrebbero essere utilizzati per nessun'altra finalità in assenza di una base giuridica ai sensi dell'articolo 6 del RGPD.

Esempio 10

un utente acquista un televisore attraverso un servizio di commercio elettronico usando un comando vocale trasmesso a un AVV. Anche se l'utente chiede successivamente la cancellazione dei propri dati, il fornitore di AVV o lo sviluppatore potrebbe comunque trattenerne alcuni in forza dell'obbligo giuridico di conservare le prove degli acquisti, come previsto dalla normativa fiscale. Tuttavia, i dati conservati a questo fine non dovrebbero eccedere la quantità minima necessaria all'adempimento dell'obbligo giuridico e non potrebbero essere trattati per nessun'altra finalità in assenza di una base giuridica ai sensi dell'articolo 6 del RGPD.

101. Come osservato nella sezione 2, le capacità di riconoscimento vocale degli AVV migliorano grazie all'addestramento dei sistemi di apprendimento automatico con i dati degli utenti. Se gli utenti non esprimono il consenso o revocano il consenso accordato all'utilizzo dei propri dati per questa finalità, i dati non potrebbero essere lecitamente utilizzati per l'addestramento di nessun altro modello e dovrebbero essere cancellati dal titolare del trattamento, sempre che non sussistano altre finalità che ne giustifichino l'ulteriore conservazione. È dimostrato, tuttavia, che alcuni modelli di apprendimento automatico possono comportare rischi di re-identificazione[35].

102. I titolari e i responsabili del trattamento dovrebbero utilizzare modelli che non limitano la loro abilità di interrompere il trattamento in caso di revoca del consenso né di agevolare il rispetto dei diritti degli interessati. I titolari e i responsabili del trattamento dovrebbero adottare misure di attenuazione per contenere il rischio di re-identificazione al di sotto di una soglia accettabile.

103. Nel caso in cui l'utente revochi il proprio consenso, i dati raccolti presso tale utente non possono più essere utilizzati per l'ulteriore addestramento del modello. Nondimeno, non è necessario eliminare il modello addestrato in precedenza con tali dati. Il CEPD sottolinea, tuttavia, che è dimostrato che alcuni modelli di apprendimento automatico comportano rischi di diffusione non autorizzata di dati personali: in particolare, numerosi studi hanno rivelato che possono essere condotti attacchi di ricostruzione e inferenza sull'appartenenza, che permettono agli autori di procurarsi informazioni sulle persone fisiche[36]. I titolari e i responsabili del trattamento dovrebbero dunque adottare misure di attenuazione per contenere il rischio

di re-identificazione al di sotto di una soglia accettabile così da accertarsi di utilizzare modelli non contenenti dati personali.

104. Gli interessati non dovrebbero essere sollecitati a conservare i propri dati indefinitamente. Poiché la cancellazione dei dati vocali o delle trascrizioni archiviati potrebbe avere un impatto sulla prestazione del servizio, tale impatto dovrebbe essere spiegato agli utenti in modo chiaro e misurabile. I fornitori di servizi di AVV dovrebbero evitare affermazioni generiche sul degrado del servizio dopo la cancellazione dei dati personali.

105. Una difficoltà particolare è rappresentata dall'anonimizzazione delle registrazioni vocali, perché è possibile identificare gli utenti grazie al contenuto del messaggio e alle caratteristiche della voce. Nondimeno, sono in corso alcune ricerche[37] sulle tecniche che potrebbero consentire di escludere informazioni situazionali, come i rumori di sottofondo, e di anonimizzare la voce.

Raccomandazioni

106. Dalla prospettiva dell'utente, lo scopo principale del trattamento dei suoi dati consiste nel porre interrogazioni e ricevere risposte e/o attivare azioni come la riproduzione di brani musicali o l'accensione/lo spegnimento di luci. Dopo che è stata data risposta a un'interrogazione o è stato eseguito un comando, i dati personali dovrebbero essere cancellati, a meno che il progettista dell'AVV o lo sviluppatore disponga di una base giuridica valida per conservarli per una finalità specifica.

107. Prima di considerare l'anonimizzazione come uno strumento per adempiere al principio di limitazione della conservazione dei dati, i fornitori di AVV e gli sviluppatori dovrebbero accertarsi che il procedimento di anonimizzazione renda la voce non identificabile.

108. Le configurazioni predefinite dovrebbero tenere conto di questi requisiti impostando in maniera predefinita la quantità minima assoluta di informazioni sull'utente che possono essere conservate. Se queste opzioni sono presentate nel contesto di un ausilio per la configurazione guidata, le impostazioni predefinite dovrebbero tenerne conto e tutte le opzioni dovrebbero essere presentate come possibilità paritarie senza discriminazione visiva.

109. Qualora, durante il procedimento di revisione, il fornitore di AVV o lo sviluppatore rilevi una registrazione originata a seguito di un'attivazione erronea, la registrazione e tutti i dati ad essa associati dovrebbero essere immediatamente cancellati e non potranno essere usati per nessuna finalità.

3.7 SICUREZZA

110. Per trattare i dati personali in sicurezza, gli AVV dovrebbero proteggerne la riservatezza, l'integrità e la disponibilità. Oltre ai rischi derivanti dagli elementi contenuti nell'ambiente dell'AVV, l'uso della voce come mezzo di comunicazione comporta una nuova serie di rischi per la sicurezza.

111. Gli AVV sono multiutenti. Possono avere più di un utente registrato e chiunque si trovi nelle loro vicinanze può emettere comandi e usare i loro servizi. Qualsiasi servizio di AVV che richieda riservatezza comporterà un meccanismo di controllo dell'accesso e l'autenticazione degli utenti. Senza il controllo dell'accesso, chiunque sia in grado di rivolgere comandi vocali all'AVV potrebbe accedere ai dati personali dell'utente, modificarli o cancellarli (ad esempio chiedere i messaggi ricevuti, l'indirizzo dell'utente o il calendario degli eventi). L'emissione di comandi vocali all'AVV non necessita della vicinanza fisica al dispositivo perché tali comandi possono essere manipolati, tra l'altro, mediante la trasmissione di segnali (ad esempio radio o televisione)[38]. Alcuni dei metodi noti per inviare comandi da remoto agli AVV, come le onde laser[39] o le onde a ultrasuoni (non udibili)[40], non sono percepibili dai sensi umani.

112. L'autenticazione dell'utente può basarsi su uno o più dei seguenti fattori: qualcosa che l'utente conosce (come una password), qualcosa che l'utente possiede (come una smart card) o qualcosa che l'utente è (come un'impronta vocale). Un esame più attento di questi fattori di autenticazione nel contesto dell'AVV indica che:

- l'autenticazione per mezzo di qualcosa che l'utente conosce è problematica; infatti, l'informazione segreta che permetterebbe all'utente di provare la propria identità dovrebbe essere pronunciata a voce alta, e verrebbe quindi rivelata a chiunque si trovi nelle vicinanze. Il canale di comunicazione degli AVV è l'aria, ossia un canale che non può essere reso più sicuro, diversamente dai canali tradizionali (ad esempio limitando l'accesso al canale o cifrandone il contenuto);
- l'autenticazione mediante qualcosa che l'utente possiede costringerebbe i fornitori del servizio di AVV a creare, distribuire e gestire «token» che potrebbero essere utilizzati come prova dell'identità;
- l'autenticazione mediante qualcosa che l'utente è implica l'uso di dati biometrici a fini di identificazione univoca di una persona fisica (si veda di seguito la sezione 3.7).

113. Gli account utente per gli AVV sono associati alle apparecchiature in cui il servizio è erogato. Spesso l'account usato per gestire l'AVV è lo stesso che viene utilizzato per gestire altri servizi. Ad esempio, i proprietari di un telefono mobile Android e di un altoparlante Google Home possono associare, e molto probabilmente assoceranno, il proprio account Google a entrambi i dispositivi. La maggior parte degli AVV non richiede né offre un meccanismo di identificazione o autenticazione quando un dispositivo che fornisce un servizio di AVV ha un solo account utente.

114. Quando, invece, al dispositivo è associato più di un account utente, alcuni AVV offrono come opzione un controllo basilare dell'accesso sotto forma di un PIN, senza alcuna vera autenticazione dell'utente, mentre altri AVV offrono l'opzione di ricorrere al riconoscimento dell'impronta vocale come meccanismo di identificazione.

115. Anche se l'identificazione o l'autenticazione dell'utente non è sempre ne-

cessaria per accedere a tutti i servizi dell'AVV, tale requisito vale senz'altro per alcuni di essi. Senza un meccanismo di identificazione o autenticazione, chiunque potrebbe avere accesso ai dati di altri utenti e modificarli o cancellarli a proprio piacimento. Ad esempio, chiunque sia vicino a un altoparlante intelligente potrebbe cancellare l'elenco dei brani preferiti di altri utenti dal servizio di streaming musicale, oppure i comandi dalla relativa cronologia o i contatti dal relativo elenco.

116. La maggior parte degli AVV si fida ciecamente delle proprie reti locali. Qualsiasi dispositivo compromesso presente nella stessa rete potrebbe modificare le impostazioni dell'altoparlante intelligente oppure autorizzare l'installazione di malware o l'associazione di applicazioni/abilità false senza il consenso e a insaputa dell'utente[41].

117. Anche gli AVV, come qualsiasi altro software, sono soggetti alle vulnerabilità tipiche dei software. Tuttavia, data la concentrazione che caratterizza il mercato degli AVV[42], qualsiasi vulnerabilità potrebbe interessare milioni di utenti di AVV. Quando funzionano nelle loro attuali modalità di progettazione, gli AVV non inviano informazioni al servizio in cloud di riconoscimento del parlato fino a quando non è rilevata l'espressione di attivazione. Tuttavia, un aggressore potrebbe sfruttare le vulnerabilità dei software per aggirare le impostazioni dell'AVV e le misure di sicurezza allo scopo, ad esempio, di fare una copia di tutti i dati inviati al cloud dell'AVV e di trasmetterli a un server sotto il proprio controllo.

118. I dati lecitamente trattati o ricavati dagli AVV permettono di realizzare un profilo piuttosto accurato dei loro utenti perché l'AVV sa o può dedurre il luogo, le relazioni e gli interessi dei propri utenti. Considerato che gli AVV sono sempre più presenti nelle case e negli smartphone degli utenti, aumenta il rischio di una sorveglianza di massa e di una profilazione di massa. Pertanto, le misure di sicurezza volte a proteggere sia i dati in transito sia quelli a riposo, nei dispositivi e nel cloud, dovrebbero essere adeguate a tali rischi.

119. L'utilizzo crescente di AVV in combinazione con un approccio non adeguatamente bilanciato all'esercizio di accessi da parte delle autorità di contrasto potrebbe generare un effetto dissuasivo tale da compromettere diritti fondamentali come la libertà di parola.

120. Le autorità di contrasto, sia nell'UE[43] che al di fuori dell'UE[44], hanno già manifestato interesse ad avere accesso ai frammenti vocali captati dagli AVV. L'accesso ai dati trattati o ricavati dagli AVV nell'UE dovrebbe essere conforme al vigente quadro normativo dell'UE in materia di protezione dei dati e tutela della vita privata. Nel caso in cui alcuni Stati membri valutino di adottare una normativa specifica che limiterebbe i diritti fondamentali alla protezione dei dati e alla tutela della vita privata, le conseguenti restrizioni dovrebbero essere in ogni caso conformi al requisito di cui all'articolo 23 dell'RGPD[45].

121. La revisione umana delle registrazioni vocali e dei dati associati per migliorare la qualità del servizio degli AVV è una prassi comune tra i fornitori di

AVV. Poiché i dati trattati dai revisori umani sono sensibili e questo procedimento è spesso subappaltato a responsabili del trattamento, è della massima importanza che siano attuate misure di sicurezza adeguate.

Raccomandazioni

122. I progettisti di AVV e gli sviluppatori di applicazioni dovrebbero mettere a disposizione degli utenti procedure di autenticazione sicure e conformi allo stato dell'arte.
123. I revisori umani dovrebbero sempre ricevere i dati strettamente necessari in forma pseudonimizzata. Gli accordi legali che disciplinano la revisione dovrebbero vietare espressamente qualsiasi trattamento che possa portare all'identificazione dell'interessato.
124. Se l'AVV offre il servizio di chiamate d'emergenza, dovrebbe essere garantito un periodo di funzionamento stabile[46].

3.8 TRATTAMENTI RIGUARDANTI CATEGORIE PARTICOLARI DI DATI

125. Come già rilevato, gli AVV hanno accesso a informazioni di natura privata che possono essere protette a norma dell'articolo 9 del RGPD (si veda la sezione 3.7.1), come i dati biometrici (si veda la sezione 3.7.2). Pertanto i progettisti di AVV e gli sviluppatori devono individuare accuratamente in quali casi il trattamento coinvolge categorie particolari di dati.

3.8.1 CONSIDERAZIONI GENERALI SUL TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI

126. Gli AVV possono trattare categorie particolari di dati in circostanze differenti:
    - quando, nell'ambito dei propri servizi, gli AVV gestiscono gli appuntamenti medici nelle agende degli utenti;
    - quando, agendo da interfaccia per servizi di terzi, i fornitori di AVV trattano il contenuto dei comandi. A seconda del tipo di servizio richiesto dall'utente, i fornitori di AVV potrebbero trattare categorie particolari di dati, ad esempio quando un utente rivolge all'AVV comandi per usare un'applicazione di terzi che tiene traccia dell'ovulazione[47];
    - quando si utilizzano dati vocali a fini di identificazione univoca dell'utente, come spiegato di seguito.

3.8.2 CONSIDERAZIONI GENERALI SUL TRATTAMENTO DEI DATI BIOMETRICI

127. Alcuni AVV hanno la capacità di individuare in modo univoco i propri utenti semplicemente sulla base della voce. Questo processo è detto «riconosci-

mento del modello vocale». Durante la fase di registrazione del riconoscimento vocale, l'AVV tratta la voce dell'utente per creare un modello vocale (o impronta vocale). Durante l'uso normale, l'AVV è in grado di calcolare il modello vocale di qualsiasi utente e di confrontarlo con i modelli registrati, per individuare in modo univoco l'utente che ha impartito un comando.

Esempio 11

un gruppo di utenti installa un AVV per usare il riconoscimento del modello vocale. Poi ciascun utente registra il proprio modello vocale.

Successivamente, un utente chiede all'AVV di accedere alle riunioni incluse nella propria agenda. Poiché l'accesso all'agenda è subordinato all'identificazione dell'utente, l'AVV estrae il modello dalla voce del richiedente, calcola il suo modello vocale e verifica se esso corrisponde a un utente registrato e se quello specifico utente ha accesso all'agenda.

128. Nell'esempio proposto, il riconoscimento della voce di un utente sulla base di un modello vocale si configura come un trattamento di categorie particolari di dati ai sensi dell'articolo 9 del RGPD (trattamento di dati biometrici a fini di identificazione univoca di una persona fisica)[48]. Il trattamento di dati biometrici a fini di identificazione dell'utente come previsto nell'esempio citato richiede il consenso esplicito dell'interessato o degli interessati in questione [articolo 9, paragrafo 2, lettera a), del RGPD]. Pertanto, quando ottengono il consenso degli utenti, i titolari del trattamento devono soddisfare le condizioni dell'articolo 7 e agire secondo le modalità specificate nel considerando 32 del RGPD; inoltre, dovrebbero offrire un metodo di identificazione alternativo a quello fondato su elementi biometrici, tenendo conto della natura volontaria del consenso.

129. Quando utilizzano dati vocali per l'identificazione biometrica o l'autenticazione, i titolari del trattamento devono indicare in modo trasparente in quali casi utilizzano l'identificazione biometrica e in che modo le impronte vocali (modelli biometrici) sono archiviate e propagate attraverso i dispositivi. Per soddisfare questo requisito di trasparenza, il CEPD raccomanda di rispondere ai seguenti interrogativi:

- l'attivazione dell'identificazione vocale in un dispositivo implementa automaticamente questa funzione anche in tutti gli altri dispositivi collegati al medesimo account?
- L'attivazione dell'identificazione vocale si propaga ai dispositivi di proprietà di altri utenti attraverso l'infrastruttura del titolare del trattamento dell'AVV?
- Dove vengono generati, archiviati e confrontati i modelli biometrici?
- I modelli biometrici sono accessibili ai fornitori di AVV, agli sviluppatori o ad altri soggetti?

130. Quando l'utente registrato configura gli AVV per identificare la voce degli utenti, anche la voce degli utenti non registrati e di quelli accidentali è trattata a fini di identificazione univoca.

131. Infatti, la rilevazione della voce del parlante in questione comporta anche il raffronto con la voce di altre persone presenti nelle vicinanze dell'assistente. In altre parole, la funzione di riconoscimento del parlante implementata negli assistenti vocali può avere bisogno di registrare le caratteristiche biometriche della voce di altri parlanti nello stesso ambiente, per poter distinguere le caratteristiche vocali del singolo utente da quelle della persona che intende essere riconosciuta. Pertanto, l'identificazione biometrica può comportare che persone non informate siano oggetto di un trattamento biometrico a seguito della registrazione del loro modello e del suo successivo confronto con quello dell'utente che intende essere riconosciuto.

132. Per evitare la raccolta di dati biometrici all'insaputa degli interessati e, allo stesso tempo, consentire a un utente di essere riconosciuto dall'assistente, si dovrebbe dare priorità alle soluzioni basate unicamente sui dati dell'utente. In termini concreti, ciò significa che il riconoscimento biometrico è attivato soltanto ad ogni utilizzo su iniziativa dell'utente, non a seguito di un'analisi permanente delle voci ascoltate dall'assistente. Ad esempio, per ottenere il consenso delle persone presenti all'avvio del trattamento biometrico si potrebbe ricorrere a una parola chiave o una domanda specifica. In tal caso, il trattamento biometrico sarebbe attivato dopo che l'utente ha pronunciato la parola «identificazione» o l'assistente ha chiesto «vuoi essere identificato?» e ha ricevuto una risposta affermativa.

> Esempio 12
>
> se l'utente vuole impostare l'autenticazione biometrica per l'accesso a taluni dati protetti, come il proprio conto bancario, l'assistente vocale potrebbe iniziare la verifica del parlante soltanto quando questi avvia l'applicazione, e verificare la sua identità in questo modo.

Raccomandazioni

133. I modelli vocali dovrebbero essere generati, archiviati e confrontati esclusivamente sul dispositivo locale, non su server remoti.

134. Vista la natura sensibile delle impronte vocali, si dovrebbero applicare scrupolosamente norme quali la ISO/IEC 24745 e tecniche di protezione dei modelli biometrici[49].

135. I fornitori di AVV che utilizzano l'identificazione biometrica basata sulla voce dovrebbero:

- garantire che l'identificazione sia sufficientemente accurata per associare in modo affidabile i dati personali agli interessati corretti;
- garantire che l'accuratezza sia simile per tutti i gruppi di utenti, verifican-

do a tal fine che non sussistano pregiudizi rilevanti nei confronti di gruppi demografici diversi.

3.9 MINIMIZZAZIONE DEI DATI

136. I titolari del trattamento dovrebbero ridurre al minimo la quantità di dati che vengono raccolti direttamente o indirettamente e ottenuti mediante trattamenti e analisi, ad esempio evitando di eseguire analisi della voce dell'utente o di altre informazioni udibili per ricavarne informazioni sullo stato mentale ovvero su possibili patologie o circostanze della vita dell'utente.
137. Si dovrebbero adottare impostazioni predefinite in grado di limitare la raccolta e/o il trattamento di dati alla quantità minima necessaria per erogare il servizio.
138. A seconda del luogo, del contesto d'uso e della sensibilità del microfono, l'AVV potrebbe raccogliere i dati vocali di terzi come parte del rumore di fondo nel momento in cui raccoglie la voce degli utenti. Anche se non comprende dati vocali, il rumore di fondo può comunque includere dati situazionali che potrebbero essere trattati per ricavarne informazioni sull'interessato (ad esempio il luogo).

Raccomandazioni

139. I progettisti di AVV dovrebbero valutare l'opportunità di usare tecnologie in grado di cancellare il rumore di fondo, per evitare di registrare e trattare le voci in sottofondo e le informazioni situazionali.

3.10 RESPONSABILIZZAZIONE

140. Per qualsiasi trattamento basato sul consenso, i titolari del trattamento devono essere in grado di dimostrare che l'interessato ha prestato il proprio consenso a norma dell'articolo 7, paragrafo 1, del RGPD. I dati vocali possono essere usati per dimostrare il rispetto del principio di responsabilizzazione (ad esempio per provare la manifestazione del consenso). L'obbligo di conservare questi dati vocali sarebbe quindi imposto dai requisiti di responsabilizzazione di cui alla pertinente legislazione specifica.
141. Rispetto alla necessità di una valutazione d'impatto sulla protezione dei dati, il CEPD ha stabilito i criteri[50] che le autorità per la protezione dei dati devono applicare quando creano elenchi delle operazioni di trattamento per le quali tale valutazione è obbligatoria, e ha fornito esempi di trattamento che verosimilmente richiedono tale valutazione. È molto probabile che i servizi di AVV rientrino nelle categorie di trattamento e nelle condizioni per le quali è stata individuata la necessità di una valutazione d'impatto sulla protezione dei dati. In tale contesto occorre verificare se il dispositivo

stia osservando, sorvegliando o controllando gli interessati ovvero se svolga una sorveglianza sistematica su larga scala ai sensi dell'articolo 35, paragrafo 3, lettera c), se siano utilizzate «nuove tecnologie» o il trattamento riguardi dati sensibili e dati concernenti interessati vulnerabili.

142. Tutte le attività di raccolta e trattamento dei dati devono essere documentate a norma dell'articolo 30 del RGPD. Sono qui compresi tutti i trattamenti che riguardano dati vocali.

Raccomandazioni

143. Se si devono usare messaggi vocali per informare gli utenti a norma dell'articolo 13, i titolari del trattamento dovrebbero pubblicare tali messaggi sul proprio sito web affinché gli utenti e le autorità per la protezione dei dati vi possano accedere.

3.11 PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA

144. I fornitori di AVV e gli sviluppatori dovrebbero valutare la necessità di avere un utente registrato per ciascuna delle loro funzionalità. Se è evidente la necessità di avere un utente registrato per gestire un'agenda o una rubrica degli indirizzi, non è altrettanto chiaro perché l'AVV debba disporre di un utente registrato per fare una telefonata o una ricerca in Internet.

145. Come impostazione predefinita, i servizi che non necessitano di un utente identificato non dovrebbero associare ai comandi nessuno degli utenti identificati degli AVV. Un AVV che per impostazione predefinita tiene conto della protezione dei dati e della tutela della vita privata tratterebbe i dati degli utenti al solo fine di eseguire le richieste di tali utenti, senza archiviare né dati vocali né un log dei comandi eseguiti.

146. Alcune apparecchiature possono far funzionare un solo AVV, mentre altre possono scegliere tra vari AVV. I fornitori di AVV dovrebbero definire norme settoriali che consentano la portabilità dei dati a norma dell'articolo 20 del RGPD.

147. Alcuni fornitori di AVV hanno affermato che i loro dispositivi non potevano cancellare tutti i dati degli utenti nemmeno su richiesta degli interessati. I fornitori di AVV dovrebbero garantire che tutti i dati degli utenti possano essere cancellati su richiesta dell'utente a norma dell'articolo 17 del RGPD.

4. MECCANISMI PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

148. In conformità del RGPD, i titolari di trattamento che forniscono servizi di AVV devono consentire a tutti gli utenti, siano essi registrati oppure no, di esercitare i propri diritti in qualità di interessati.

149. I fornitori di AVV e gli sviluppatori dovrebbero facilitare il controllo degli interessati sui propri dati durante l'intero periodo del trattamento, in particolare agevolando l'esercizio dei loro diritti di accesso, rettifica, cancellazione, limitazione del trattamento e, a seconda della base giuridica del trattamento, alla portabilità dei dati personali e di opposizione.

150. Il titolare del trattamento dovrebbe fornire informazioni sui diritti dell'interessato nel momento in cui questi accende un AVV e, al più tardi, quando viene trattata la prima richiesta vocale dell'utente.

151. Considerato che il principale mezzo di interazione degli AVV è la voce, i progettisti di AVV dovrebbero garantire che gli utenti, siano essi registrati oppure no, possano esercitare qualsiasi diritto riconosciuto agli interessati mediante comandi vocali di facile uso. Alla fine del trattamento i progettisti di AVV – e gli sviluppatori di applicazioni, nel caso in cui possano contribuire alla soluzione – dovrebbero comunicare all'utente, mediante una comunicazione vocale, una notifica scritta inviata al telefonino o all'account dell'utente ovvero con qualsiasi altra modalità scelta dall'utente, che i suoi diritti sono stati presi in debita considerazione.

152. I progettisti di AVV e gli sviluppatori di applicazioni in particolare dovrebbero implementare quanto meno strumenti specifici che permettano di esercitare i suddetti diritti in modo efficace ed efficiente. A tal fine dovrebbero proporre nei rispettivi dispositivi una modalità per l'esercizio dei diritti degli interessati, ad esempio fornendo all'interessato strumenti self-service o un sistema di gestione del profilo[51]. Ciò potrebbe facilitare una gestione efficiente e tempestiva dei diritti degli interessati e consentirà al titolare del trattamento di includere meccanismi di identificazione nello strumento self-service.

153. Per quanto riguarda l'esercizio dei diritti degli interessati in presenza di una pluralità di utenti, l'utente, registrato o non registrato, che esercita uno dei propri diritti dovrebbe poterlo fare senza compromettere i diritti di uno qualsiasi degli altri utenti. Tutti gli utenti, siano essi registrati oppure no, possono esercitare i propri diritti fintantoché il titolare del trattamento continua a trattare i dati. Il titolare del trattamento dovrebbe istituire un procedimento atto a garantire l'esercizio dei diritti degli interessati.

4.1 DIRITTO DI ACCESSO

154. A norma dell'articolo 12, paragrafo 1, del RGPD, le comunicazioni di cui all'articolo 15 dovrebbero essere fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Per quanto riguarda l'accesso ai dati personali oggetto di trattamento, l'articolo 15, paragrafo 3, stabilisce che, se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni dovrebbero essere fornite in un formato elettronico di uso comune. Per valutare se un formato elettronico possa essere considerato di uso comune, si dovrebbe fare riferimento alle ragionevoli aspettative degli interessati, non al formato che il titolare

del trattamento utilizza nelle proprie operazioni quotidiane. L'interessato non dovrebbe essere tenuto ad acquistare software o hardware specifici per poter accedere alle informazioni.

155. Pertanto, successivamente a una richiesta, i titolari del trattamento dovrebbero inviare una copia dei dati personali e, in particolare, i dati audio (comprese le registrazioni vocali e le trascrizioni) in un formato di uso comune leggibile dall'interessato.

156. Nel decidere il tipo di formato da utilizzare per fornire le informazioni di cui all'articolo 15, il titolare del trattamento deve considerare che il formato dovrebbe permettere di presentare le informazioni in un modo che sia non solo intellegibile ma anche facilmente accessibile. I titolari del trattamento dovrebbero inoltre adattare le informazioni alla situazione specifica dell'interessato che ha presentato la richiesta.

Esempio 13

un titolare del trattamento che fornisce un servizio di AVV riceve da un utente sia una richiesta di accesso sia una richiesta di portabilità dei dati. Il titolare decide di fornire sia le informazioni a norma dell'articolo 15 sia quelle a norma dell'articolo 20 in un file PDF. In questo caso, il modo in cui il titolare del trattamento ha gestito le due richieste non dovrebbe essere considerato corretto. Un file PDF è tecnicamente conforme agli obblighi del titolare del trattamento quali previsti dall'articolo 15, ma non soddisfa gli obblighi che gli sono imposti dall'articolo 20[52].

Va rilevato che il semplice rinvio degli utenti a una cronologia delle loro interazioni con l'assistente vocale non permetterebbe al titolare del trattamento di adempiere a tutti gli obblighi in materia di diritto di accesso, poiché i dati accessibili in tal modo sono generalmente soltanto una parte delle informazioni trattate nel contesto dell'erogazione del servizio.

157. Il diritto di accesso non dovrebbe essere usato per contrastare/aggirare i principi di minimizzazione e conservazione dei dati.

4.2 DIRITTO DI RETTIFICA

158. Per agevolare la rettifica dei dati, gli utenti, siano essi registrati oppure no, dovrebbero poter gestire e aggiornare i propri dati in qualsiasi momento direttamente dal dispositivo dell'AVV, come descritto sopra. Inoltre, lo strumento self-service dovrebbe essere implementato all'interno del dispositivo o di un'applicazione affinché possa aiutare gli utenti a rettificare facilmente i propri dati personali. L'aggiornamento dovrebbe essere notificato agli utenti a voce o per iscritto.

159. Più in generale, il diritto di rettifica si applica a qualsiasi opinione e deduzione[53] del titolare del trattamento, compresa la profilazione, e dovrebbe

tenere conto del fatto che la grande maggioranza dei dati è altamente soggettiva[54].

4.3 DIRITTO DI CANCELLAZIONE

160. Gli utenti, siano essi registrati oppure no, dovrebbero poter cancellare in ogni momento i dati che li riguardano tramite un comando vocale rivolto al dispositivo dell'AVV ovvero tramite uno strumento self-service integrato in qualsiasi apparecchiatura associata all'AVV. A tal fine, i dati personali possono essere cancellati dall'interessato con la stessa facilità con cui sono comunicati. A causa delle difficoltà intrinseche nell'anonimizzazione dei dati vocali e dell'ampia gamma di dati personali raccolti presso l'interessato ovvero osservati e dedotti in merito all'interessato[55], appare difficile che, in questo contesto, il diritto di cancellazione possa essere rispettato rendendo anonimi i dati personali. Tuttavia, poiché il RGPD è tecnologicamente neutrale e le tecnologie si evolvono rapidamente, non si può escludere che in futuro il diritto di cancellazione possa essere esercitato mediante l'anonimizzazione.

161. In alcuni casi, in mancanza di uno schermo di terzi o della possibilità di visualizzare i dati archiviati (ad esempio un'applicazione mobile o un dispositivo tabulare), è difficile avere un'anteprima delle tracce registrate, al fine di valutare la rilevanza dei suggerimenti. Insieme all'assistente vocale dovrebbe essere fornito, per facilitarne l'uso, un pannello dei comandi (o un'applicazione) facilmente accessibile agli utenti allo scopo di cancellare la cronologia delle richieste e personalizzare lo strumento in base alle esigenze dell'utente[56].

162. In qualsiasi trattamento di dati e, in particolare, quando gli interessati registrati acconsentono alla trascrizione e all'uso delle registrazioni vocali da parte del fornitore al fine di migliorare i suoi servizi, i fornitori di AVV dovrebbero essere in grado, su richiesta dell'utente, di cancellare la registrazione vocale iniziale nonché ogni connessa trascrizione dei dati personali.

163. Il titolare del trattamento dovrebbe garantire che, dopo l'esercizio del diritto di cancellazione, non sia più possibile effettuare altri trattamenti. Per quanto riguarda le azioni precedenti, il diritto di cancellazione può essere sottoposto a taluni limiti, in particolare di natura giuridica e tecnica.

Esempio 14

se, prima della richiesta di cancellazione, un utente aveva effettuato un acquisto online per mezzo del proprio AVV, il fornitore dell'AVV può cancellare la registrazione vocale relativa all'acquisto online e garantire che non sia più usata in futuro. Tuttavia, l'acquisto sarà comunque valido, e lo saranno anche l'ordine vocale o la trascrizione trattata dal sito web di commercio online (in questo caso la deroga si fonda sull'obbligo giuridico

cui è soggetto il sito).

Analogamente, se prima della richiesta di cancellazione l'utente ha aggiunto uno specifico brano musicale al proprio elenco per mezzo dell'AVV, i fornitori dell'AVV potranno cancellare la richiesta orale ma non le conseguenze della stessa (la cancellazione non avrà effetti sull'elenco dei brani scelti dall'utente).

164. In considerazione di quanto sopra esposto, nel caso in cui un medesimo dato personale sia trattato per finalità di trattamento differenti, i titolari del trattamento dovrebbero interpretare le richieste di cancellazione come un chiaro segnale volto a porre fine al trattamento dei dati per tutte le finalità non giuridicamente soggette a deroga.

    In conformità delle condizioni di cui all'articolo 21, paragrafo 1, del RGPD, i dati trattati sulla base degli interessi legittimi dei fornitori di AVV non dovrebbero essere oggetto di una deroga al diritto di cancellazione, in particolare perché gli interessati ragionevolmente non si aspettano un ulteriore trattamento dei propri dati personali.

4.4 DIRITTO ALLA PORTABILITÀ DEI DATI PERSONALI

165. Il trattamento dei dati eseguito dai fornitori di AVV rientra nell'ambito di applicazione della portabilità dei dati perché le operazioni di trattamento sono basate prevalentemente sul consenso dell'interessato [a norma dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), nel caso di categorie particolari di dati] ovvero su un contratto di cui l'interessato è parte a norma dell'articolo 6, paragrafo 1, lettera b).

166. Nella pratica, il diritto alla portabilità dei dati personali dovrebbe facilitare il passaggio da un fornitore di AVV a un altro. Nel caso degli AVV che operano in particolare in un ambiente digitale, e se la voce dell'interessato è registrata in un'applicazione o su una piattaforma, il diritto alla portabilità dei dati personali dovrebbe essere garantito per tutti i dati personali forniti dall'interessato. Inoltre, il titolare del trattamento dovrebbe offrire agli utenti la possibilità di recuperare direttamente i propri dati personali dalla propria area utente, attraverso uno strumento self-service. Gli utenti dovrebbero altresì poter esercitare questo diritto anche mediante un comando vocale.

167. I fornitori di AVV e gli sviluppatori dovrebbero dare agli interessati un'ampia capacità di controllo sui dati personali che li riguardano, per consentire loro di trasferirli da un fornitore di AVV a un altro. Pertanto gli interessati dovrebbero ricevere i propri dati personali forniti al titolare del trattamento in un formato strutturato, di uso comune e leggibile da dispositivo automatico, nonché attraverso mezzi[57] che contribuiscono a rispondere alle richieste di portabilità dei dati (quali strumenti per lo scaricamento e in-

terfacce per la programmazione di applicazioni)[58]. Qualora gli insiemi di dati personali raccolti siano complessi o di grandi dimensioni – come potrebbe essere il caso qui considerato – il titolare del trattamento dovrebbe fornire, ai sensi delle linee guida sul diritto alla portabilità dei dati, una panoramica «in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro» (si veda l'articolo 12, paragrafo 1, del RGPD), in modo tale che gli interessati sappiano sempre con chiarezza quali dati devono scaricare o trasmettere a un altro titolare del trattamento in relazione a una determinata finalità. Ad esempio, gli interessati dovrebbero essere in grado di utilizzare applicazioni software per individuare, riconoscere e trattare facilmente dati specifici.

168. Questo diritto dovrebbe permettere all'utente di recuperare ad uso personale, in particolare, i dati che ha comunicato a voce (ad esempio cronologia delle interazioni vocali) e nell'ambito della creazione del proprio account utente (ad esempio nome e cognome).

169. Ai fini della completa applicazione di questo diritto dell'interessato in un contesto di mercato unico digitale, i progettisti di AVV e gli sviluppatori di applicazioni dovrebbero elaborare, in particolare, formati comuni leggibili da dispositivo automatico che agevolino l'interoperabilità dei formati di dati tra i sistemi degli AVV[59], compresi formati standard per dati vocali. Le tecnologie dovrebbero essere strutturate in modo tale da garantire che i dati personali trattati, compresi quelli vocali, possano essere facilmente e integralmente riutilizzati dal nuovo titolare del trattamento[60].

170. Per quanto attiene al formato, i fornitori di AVV dovrebbero mettere a disposizione i dati personali in formati aperti di uso comune (ad esempio mp3, wav, csv, gsm ecc.) insieme a metadati idonei, allo scopo di descrivere accuratamente il significato delle informazioni scambiate[61].

5. ALLEGATO: RICONOSCIMENTO AUTOMATICO DEL PARLATO, SINTESI DEL PARLATO E TRATTAMENTO DEL LINGUAGGIO NATURALE

171. Sulla base dei fondamenti teorici del trattamento di segnali, in particolare delle teorie di Claude Shannon sull'informazione e il campionamento, il trattamento automatico del parlato è diventato una componente fondamentale delle discipline ingegneristiche. All'incrocio tra fisica (acustica, propagazione delle onde), matematica applicata (modellizzazione, statistica), informatica (algoritmi, tecniche di apprendimento) e scienze umane (percezione, ragionamento), il trattamento del parlato ha dato ben presto origine a numerose branche di studio: identificazione e verifica del parlante, riconoscimento automatico del parlato, sintesi vocale, rilevamento di emozioni eccetera. All'incirca negli ultimi quindici anni la disciplina nel suo complesso ha compiuto progressi molto significativi grazie a vari fattori: miglioramento dei metodi di analisi, un significativo aumento delle capacità informatiche e maggiori quantità di dati disponibili.

5.1 RICONOSCIMENTO AUTOMATICO DEL PARLATO

172. Il riconoscimento automatico del parlato (detto anche «dal discorso al testo») prevedeva un tempo tre fasi distinte finalizzate a: 1) determinare quali fonemi fossero stati pronunciati usando un modello acustico; 2) determinare quali parole fossero state pronunciate utilizzando un dizionario fonetico; 3) trascrivere la sequenza di parole (frase) che con maggiore probabilità era stata pronunciata usando un modello linguistico. Grazie ai progressi resi possibili dall'apprendimento profondo (deep learning - una tecnica di apprendimento automatico), oggi molti sistemi offrono il riconoscimento automatico end-to-end del parlato, che consente di evitare il complesso apprendimento di tre modelli differenti e al tempo stesso di ottenere prestazioni migliori in termini di risultati e tempi di trattamento. Attualmente, quasi tutti i principali operatori digitali offrono proprie applicazioni per il riconoscimento automatico del parlato, che possono essere utilizzate facilmente dai sistemi di interfaccia di programmazione delle applicazioni; sono disponibili, tuttavia, anche sistemi open-source come, ad esempio, DeepSpeech[62] o Kaldi[63].

5.2 TRATTAMENTO DEL LINGUAGGIO NATURALE (NLP)

173. Il trattamento del linguaggio naturale è un ambito interdisciplinare che interessa la linguistica, l'informatica e l'intelligenza artificiale e mira a realizzare strumenti di trattamento del linguaggio naturale per molteplici applicazioni. I campi di ricerca e le applicazioni sono numerosi: analisi sintattica, traduzione automatica, generazione e sintesi automatiche di testi, controllo ortografico, sistemi di risposta a domande, text mining, riconoscimento di entità nominate, analisi del sentiment eccetera. In concreto, l'obiettivo del trattamento del linguaggio naturale è quello di dotare i computer della capacità di leggere e comprendere i linguaggi umani e di ricavarne significati. Lo sviluppo delle applicazioni di trattamento del linguaggio naturale è complesso perché tradizionalmente gli strumenti informatici hanno bisogno che gli esseri umani interagiscano con loro in un linguaggio di programmazione che è formale, preciso in termini di significato, non ambiguo e altamente strutturato. Ma il linguaggio umano non è sempre preciso: spesso è ambiguo e la struttura linguistica può dipendere da molte variabili complesse, tra cui linguaggi gergali, dialetti regionali e il contesto sociale.

174. L'analisi sintattica e quella semantica sono due delle tecniche principali usate nel trattamento del linguaggio naturale. La sintassi consiste nella collocazione delle parole all'interno di una frase affinché creino un senso grammaticale. Il trattamento del linguaggio naturale utilizza la sintassi per stabilire il significato di una lingua sulla base delle regole grammaticali. Le tecniche sintattiche impiegate comprendono la parsificazione (analisi grammaticale di una frase), la segmentazione in parole (suddivisione di un testo lungo in unità distinte), la frammentazione in frasi (separazione tra le

frasi di un testo lungo), la segmentazione morfologica (suddivisione delle parole in gruppi) e la ricerca della radice delle parole (suddivisione delle parole contenenti flessioni o desinenze nelle rispettive forme radicali). La semantica riguarda l'uso e il significato delle parole. Il trattamento del linguaggio naturale applica algoritmi per comprendere il significato e la struttura delle frasi. Le tecniche usate nel trattamento del linguaggio naturale in relazione alla semantica comprendono la disambiguazione del senso (che ricava il significato di una parola in base al contesto), il riconoscimento delle entità nominate (che individua le parole che si possono categorizzare in gruppi) e la generazione di linguaggio naturale (che utilizza una banca dati per determinare la semantica delle parole). I precedenti approcci al trattamento del linguaggio naturale utilizzavano metodi basati su regole, nei quali a semplici algoritmi di apprendimento automatico veniva ordinato di cercare determinate parole e frasi in un testo e venivano fornite risposte specifiche non appena apparivano le frasi cercate; invece, gli approcci attuali al trattamento del linguaggio naturale si basano sull'apprendimento profondo, un tipo di IA che prende in esame e usa modelli rinvenibili nei dati per migliorare la comprensione di un programma.

5.3 SINTESI DEL PARLATO

175. La sintesi del parlato consiste nella produzione artificiale di parlato umano. È stata implementata principalmente mediante la concatenazione di unità vocali archiviate in una banca dati. Tale tecnica consiste nel selezionare, fra tutte le registrazioni di un parlante precedentemente trascritte sotto forma di fonemi, sillabe e parole, gli elementi sonori corrispondenti alle parole che devono essere pronunciate dall'AVV, e nell'assemblarli uno dopo l'altro fino a formare una frase intelligibile pronunciata con una dizione naturale. In alternativa, un sintetizzatore vocale può incorporare un modello del tratto vocale e altre caratteristiche della voce umana per modellizzare i parametri di una voce, come intonazione, ritmo e timbro, mediante modelli statistici generativi quali WaveNet[64], Tacotron[65] e DeepVoice[66] e creare quindi un risultato vocale completamente sintetico.

NOTE

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in appresso «RGPD»).

[2] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), quale modificata dalla direttiva 2006/24/CE e dalla direttiva 2009/136/CE (in appresso «la direttiva e-privacy»).

[3] Nel presente documento, per «Stati membri» s'intendono gli «Stati membri del SEE».

[4] Si veda, ad esempio, il comunicato stampa del 1° agosto 2019 dell'Autorità di Amburgo per la protezione dei dati e l'informazione: https://datenschutz-hamburg.de/pressemitteilungen/2019/08/2019-08-01-google-assistant

[5] Si veda, ad esempio, qui: https://www.amazon.science/blog/alexas-new-speech-recognition-abilities-showcased-at-interspeech.

[6] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), quale modificata dalla direttiva 2006/24/CE e dalla direttiva 2009/136/CE (in appresso «la direttiva e privacy»).

[7] L'articolo 1 della direttiva 2008/63/CE della Commissione, del 20 giugno 2008, relativa alla concorrenza sui mercati delle apparecchiature terminali di telecomunicazione, definisce le «apparecchiature terminali» come «a) le apparecchiature allacciate direttamente o indirettamente all'interfaccia di una rete pubblica di telecomunicazioni per trasmettere, trattare o ricevere informazioni; in entrambi i casi di allacciamento, diretto o indiretto, esso può essere realizzato via cavo, fibra ottica o via elettromagnetica; un allacciamento è indiretto se l'apparecchiatura è interposta fra il terminale e l'interfaccia della rete pubblica; b) apparecchiature delle stazioni terrestri di comunicazione via satellite;».

[8] Si vedano le linee guida 1/2020 del CEPD, paragrafo 12, per un ragionamento analogo sui veicoli connessi (in appresso «linee guida CEPD 1/2020»). Si veda anche il parere 5/2019 sull'interazione tra la direttiva e-privacy e il regolamento generale sulla protezione dei dati, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati del CEPD.

[9] Ibidem, paragrafo 41.

[10] Parere 5/2019, paragrafo 41.

[11] CEPD, Linea guida 2/2019 sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, versione 2.0, 8 ottobre 2019, paragrafo 1.

[12] È possibile che i dispositivi di AVV futuri adottino il metodo dell'elaborazione al margine della rete e possano quindi fornire alcuni servizi a livello locale. In tal caso sarà necessario riconsiderare l'applicabilità della direttiva e-privacy.

[13] Si vedano anche le linee guida 1/2020 del CEPD, paragrafo 14.

[14] L'articolo 4, punto 14, del RGPD definisce i dati biometrici come «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici».

[15] Si pensi, per esempio, all'ambiente domestico, a un veicolo, una strada, al luogo di lavoro o a qualsiasi altro spazio privato, pubblico o professionale, ovvero a una combinazione di tali spazi.

[16] L'articolo 4, punto 1, del RGPD specifica altresì che «si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

[17] L'articolo 9, paragrafo 1, del RGPD definisce le categorie particolari di dati personali come «i

dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché [...] dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona» e ne vieta il trattamento.

[18] Linee guida CEPD 7/2020 sui concetti di titolare e responsabile del trattamento di cui al RGPD, versione 2.0, adottate il 7 luglio 2021 (in appresso «linee guida 7/2020»).

[19] Articoli 12-14 e articolo 26 del RGPD.

[20] Linee guida 7/2020, paragrafo 165.

[21] Si vedano le linee guida 4/2019 del CEPD sull'articolo 25 relativo alla protezione dei dati fin dalla progettazione e per impostazione predefinita, versione 2.0, adottate il 20 ottobre 2020.

[22] Linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679, WP260, revisione 01, approvate dal CEPD (in appresso «linee guida WP260 del GL 29»), paragrafo 11.

[23] Linee guida WP260 del GL 29, paragrafo 19.

[24] Linee guida WP260 del GL 29, paragrafo 21.

[25] Articolo 4, punto 11, del RGPD.

[26] Eoghan Furey, Juanita Blue, «Alexa, Emotion, Privacy and GDPR» (Alexa, emozione, tutela della vita privata e RGPD), relazione per la Human Computer Interaction Conference, luglio (2018).

[27] A condizione che sia dimostrata «la validità del contratto ai sensi del diritto contrattuale nazionale applicabile», come rilevato nel paragrafo 26 delle linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati (in appresso «le linee guida 2/2019»).

[28] In conformità delle linee guida 2/2019, in cui si afferma altresì che il parere 06/2014 resta pertinente per l'articolo 6, paragrafo 1, lettera b), e il RGPD (si vedano in particolare le pagine 11, 16, 17, 18 e 55 di tale parere).

[29] Si vedano le linee guida 2/2019, rispettivamente i paragrafi 18, 19, 20, 21 e 27.

[30] Dal punto di vista tecnico, il concetto di «identificazione» va distinto da quello di «verifica» (autenticazione). L'identificazione consiste in una ricerca e un confronto «uno contro tanti» (1: N) e richiede, in linea di principio, una banca dati in cui sono elencate numerose persone fisiche. Invece il trattamento per finalità di verifica è un confronto «uno contro uno» (1:1) ed è utilizzato per verificare e confermare mediante comparazione biometrica se una persona è la stessa da cui hanno origine i dati biometrici presentati. Per quanto di conoscenza del CEPD, gli AVV disponibili sul mercato si basano esclusivamente sull'impiego di tecnologie di identificazione del parlante.

[31] Il RGPD ritiene che la mera natura di «dato» non sia sempre sufficiente per stabilire se esso debba essere considerato appartenente a una categoria particolare di dati, visto che, nel trattamento di fotografie, esse «rientrano nella definizione di dati biometrici soltanto quando siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica» (considerando 51). Lo stesso ragionamento vale per la voce.

[32] Si vedano anche le linee guida 2/2019, paragrafo 57.

[33] Si vedano le linee guida 05/2020 sul consenso ai sensi del regolamento (UE) 2016/679 del CEPD, adottate il 4 maggio 2020, sezione 3.2.

[34] Si veda la lettera di Amazon del 28 giugno 2019 in risposta al senatore statunitense Christopher Coons: https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons__Response%20Letter__6.28.19[3].pdf.

[35] Veale Michael, Binns Reuben ed Edwards Lilian, 2018, «Algorithms that remember: model inversion attacks and data protection law» (Algoritmi che ricordano: attacchi di inversione dei modelli e norme sulla protezione dei dati), Phil. Trans. R. Soc. A.37620180083, doi: 10.1098/rsta.2018.0083.

[36] N. Carlini et al., «Extracting Training Data from Large Language Models» (Estrarre dati per l'addestramento da grandi modelli di linguaggio), dicembre 2020.

[37] Si veda, ad esempio, VoicePrivacy (https://www.voiceprivacychallenge.org), un'iniziativa intesa sviluppare soluzioni in grado di mantenere la riservatezza per la tecnologia vocale.
Si vedano anche gli strumenti di anonimizzazione della voce open-source sviluppati dal progetto di ricerca e innovazione COMPRISE del programma Orizzonte 2020: https://gitlab.inria.fr/comprise/voice_transformation.

[38] X. Yuan et al., «All Your Alexa Are Belong to Us: A Remote Voice Control Attack against Echo» (Tutte le vostre Alexa appartengono a noi: un attacco di controllo remoto della voce contro Echo), 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, Emirati arabi uniti, 2018, pagg. 1-6, doi: 10.1109/

GLOCOM.2018.8647762.

[39] Si veda, per esempio, https://lightcommands.com.

[40] Si veda, per esempio, https://surfingattack.github.io.

[41] Si veda, ad esempio, Deepak Kumar et al., *Skill Squatting Attacks on Amazon Alexa* (Attacchi di occupazione di abilità contro Alexa di Amazon), USENIX Security Symposium, agosto 2018, https://www.usenix.org/conference/usenixsecurity18/presentation/kumar.
Security Research Labs, *Smart Spies: Alexa and Google Home expose users to vishing and eavesdropping* (Spie intelligenti: Alexa e Google Home espongono gli utenti a vishing e origliamento), novembre 2019, https://srlabs.de/bites/smart-spies.

[42] Attualmente il mercato degli AVV è suddiviso tra meno di una dozzina di fornitori di questi servizi.

[43] Si veda, per esempio, https://www.ft.com/content/ad765972-87a2-11e9-a028-86cea8523dc2.

[44] Si veda, per esempio, https://cdt.org/insights/alexa-is-law-enforcement-listening.

[45] Si vedano anche le linee guida 10/2020 del CEPD sulle restrizioni di cui all'articolo 23 del RGPD.

[46] È il periodo di tempo in cui un dispositivo o un servizio possono essere lasciati incustoditi senza che vadano in blocco o debbano essere riavviati per l'amministrazione o la manutenzione.

[47] Si veda, per esempio, un prodotto disponibile a questo indirizzo: https://www.amazon.com/Ethan-Fan-Ovulation-Period-Tracker/dp/B07CRLSHKY.

[48] Ndr. La nota non è stata inserita, per errore, nella versione ufficiale delle Linee guida.

[49] Si vedano, ad esempio:
Jain, Anil e Nandakumar, Karthik e Nagar, Abhishek, 2008, *Biometric Template Security* (Sicurezza dei modelli biometrici), EURASIP Journal on Advances in Signal Processing, 2008, 10.1155/2008/579416.
S. K. Jami, S. R. Chalamala e A. K. Jindal, *Biometric Template Protection Through Adversarial Learning* (Protezione dei modelli biometrici mediante l'apprendimento automatico in ambiente ostile), 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2019, pagg. 1-6, doi: 10.1109/ICCE.2019.8661905.

[50] Gruppo di lavoro Articolo 29, Linee guida in materia di valutazione d'impatto sulla protezione dei dati, WP248, revisione 01, approvate dal CEPD.

[51] Per «sistema di gestione del profilo» s'intende un'area all'interno del sistema dell'AVV in cui gli utenti possono in qualsiasi momento archiviare le proprie preferenze, impostare modifiche e modificare facilmente le proprie impostazioni per la tutela della vita privata.

[52] Linee guida del gruppo di lavoro Articolo 29 sul diritto alla portabilità dei dati, approvate dal CEPD, pag. 18.

[53] Il fatto che le opinioni e le deduzioni possano essere considerate dati personali è stato confermato dalla CGUE, che ha osservato come l'espressione «qualsiasi informazione» nella definizione dei dati personali comprende informazioni «tanto oggettive quanto soggettive, sotto forma di pareri o di valutazioni, a condizione che esse siano "concernenti" la persona interessata» (causa C-434/16 *Peter Nowak/Garante per la protezione dei dati personali*, ECLI:EU:C:2017:994, punto 34).

[54] Getting Data Subject Rights Right (Attuare correttamente i diritti degli interessati), testo sottoposto al CEPD da studiosi della protezione dei dati, novembre 2019.

[55] Parere 05/2014 del gruppo di lavoro Articolo 29 sulle tecniche di anonimizzazione, adottato il 10 aprile 2014.

[56] «Assistants vocaux et enceintes connectées, l'impact de la voix sur l'offre et les usages culturels et médias», Conseil Supérieur de l'Audiovisuel della Francia, maggio 2019.

[57] Si veda, a titolo di spiegazione, il ragionamento del gruppo di lavoro Articolo 29 riportato nelle linee guida sul diritto alla portabilità dei dati, approvate dal CEPD, pag. 16:
«Sul piano tecnico, i titolari dovrebbero esplorare e valutare due approcci diversi e complementari per mettere a disposizione degli interessati o di altri titolari dati che siano portabili:
- trasmissione diretta dell'intero insieme di dati portabili (o di più estratti di parti del set complessivo di dati);
- utilizzo di uno strumento automatizzato che consenta l'estrazione dei dati pertinenti.

Il secondo approccio sarà forse preferibile per quei titolari che hanno a che fare con insiemi complessi e di grandi dimensioni, in quanto permette di estrarre quelle parti del set di dati che sono pertinenti per l'interessato nel contesto della sua specifica richiesta, può favorire la minimizzazione del rischio, e probabilmente consente il ricorso a meccanismi di sincronizzazione dei dati – per esempio, nel contesto di comunicazioni regolari fra titolari del trattamento. Si tratta di un approccio forse più idoneo a garantire l'osservanza delle norme da parte del "nuovo" titolare, e potrebbe configurare una buona prassi per ridurre i rischi in termini di privacy da parte del titolare iniziale.».

[58] Si vedano a questo proposito le linee guida del gruppo di lavoro Articolo 29 sul diritto alla portabilità dei dati, approvate dal CEPD, pag. 1.

[59] Si vedano a questo proposito il considerando 68 del RGPD e le linee guida del gruppo di lavoro Articolo 29 sul diritto alla portabilità dei dati, approvate dal CEPD, pag. 17.

[60] «In questo senso, il considerando 68 promuove lo sviluppo di formati interoperabili da parte dei titolari così da consentire la portabilità dei dati, ma non configura un obbligo in capo ai titolari stessi di introdurre o mantenere sistemi di trattamento tecnicamente compatibili. Tuttavia, il RGPD vieta ai titolari di creare ostacoli alla trasmissione dei dati.», come stabilito nelle linee guida del gruppo di lavoro Articolo 29 sul diritto alla portabilità dei dati, approvate dal CEPD, pag. 5.

[61] Il CEPD incoraggia vivamente la cooperazione tra le parti interessate del settore e le associazioni di categoria affinché elaborino congiuntamente un insieme comune di norme e formati interoperabili per soddisfare i requisiti del diritto alla portabilità dei dati.

[62] https://github.com/mozilla/DeepSpeech.

[63] https://github.com/kaldi-asr/kaldi.

[64] Aäron van den Oord e Sander Dieleman, *WaveNet: A generative model for raw audio* (WaveNet: un modello generativo per audio grezzi), blog Deepmind, settembre 2016, https://deepmind.com/blog/article/wavenet-generative-model-raw-audio

[65] Yuxuan Wang, Expressive *Speech Synthesis with Tacotron* (Sintesi espressiva del parlato con Tacotron), blog Google AI, marzo 2018, https://ai.googleblog.com/2018/03/expressive-speech-synthesis-with.html

[66] *Deep Voice 3: 2000-Speaker Neural Text-to-Speech*, blog Baidu Research, ottobre 2017, http://research.baidu.com/Blog/index-view?id=91

Raccomandazioni 02/2021 sulla base giuridica per la conservazione dei dati delle carte di credito al solo scopo di agevolare ulteriori operazioni online

Adottate il 19 maggio 2021

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in appresso: il «RGPD»),

visto l'accordo SEE e in particolare l'allegato XI e il protocollo 37 dello stesso, come modificato dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018,

visti gli articoli 12 e 22 del proprio regolamento interno,

HA ADOTTATO LE SEGUENTI RACCOMANDAZIONI:

1. Nel contesto della pandemia di COVID-19 l'economia digitale e il commercio elettronico hanno continuato a svilupparsi. Analogamente, si sono acutizzati i rischi connessi all'utilizzo online dei dati delle carte di credito. Come affermato dal gruppo di lavoro «Articolo 29» nelle sue linee guida in materia di valutazione d'impatto sulla protezione dei dati, la violazione dei dati delle carte di credito «*implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato» in quanto i dati finanziari possono essere utilizzati per «frodi relative ai pagamenti*»[1].
2. È pertanto essenziale che i titolari del trattamento mettano in atto adeguate garanzie per gli interessati e garantiscano loro il controllo sui rispettivi dati personali, così da ridurre il rischio di trattamenti illeciti e promuovere la fiducia nell'ambiente digitale. L'EDPB ritiene che tale fiducia sia essenziale per la crescita sostenibile dell'economia digitale.
3. A tal fine, le presenti raccomandazioni mirano a promuovere un'applicazione armonizzata delle norme sulla protezione dei dati per quanto riguarda il trattamento dei dati delle carte di credito all'interno dello Spazio economico europeo (SEE) e a garantire una protezione omogenea dei diritti degli interessati, nel pieno rispetto dei principi fondamentali in materia di protezione dei dati, come richiesto dal RGPD.
4. Più specificamente, le presenti raccomandazioni riguardano la conservazione dei dati delle carte di credito da parte dei fornitori di prodotti e servizi online al solo scopo specifico di facilitare ulteriori acquisti da parte degli interessati[2]. Esse riguardano la situazione in cui un interessato acquista un prodotto o paga un servizio tramite un sito web o un'applicazione e fornisce i dati della propria carta di credito, generalmente su un apposito modulo, al fine di concludere questa singola operazione.
5. Come sempre, il titolare del trattamento deve disporre di una base giuridica valida ai sensi dell'articolo 6 del RGPD per conservare tali dati. Al riguardo, va osservato che alcune delle basi giuridiche di cui all'articolo 6 del RGPD non sarebbero applicabili alla situazione in esame e devono essere escluse. La conservazione dei dati della carta di credito successivamente a una transazione, al fine di facilitare ulteriori acquisti, non può essere considerata necessaria per l'adempimento di un obbligo legale [articolo 6, paragrafo 1, lettera c), RGPD] né per la salvaguardia degli interessi vitali di una persona fisica [articolo 6, paragrafo 1, lettera d), RGPD]. Nemmeno l'esercizio di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento [articolo 6, paragrafo 1, lettera e), RGPD] può essere considerata una base giuridica idonea.
6. Inoltre, la conservazione dei dati della carta di credito dopo il pagamento di prodotti o servizi non è, in quanto tale, necessaria per l'esecuzione di un contratto [articolo 6, paragrafo 1, lettera b), RGPD]. Mentre, in primo luogo, il trattamento dei dati relativi alla carta di credito utilizzata dal cliente per pagare è necessario per l'esecuzione del contratto, rendendo così applicabile l'articolo 6, paragrafo 1, lettera b), RGPD, la conservazione di tali dati è utile solo per agevolare una potenziale successiva operazione di pagamento e fa-

cilitare le vendite. Tale finalità non può essere considerata strettamente necessaria all'esecuzione del contratto per la fornitura del prodotto o servizio che l'interessato ha già pagato[3].

7. Per quanto riguarda il trattamento necessario ai fini del legittimo interesse del titolare o di un terzo[4], il comitato osserva che, affinché il titolare del trattamento possa invocare l'articolo 6, paragrafo 1, lettera f), RGPD, devono essere soddisfatte le tre condizioni stabilite dal medesimo articolo[5]. Tale base giuridica richiede, in primo luogo, l'individuazione e la qualificazione di un legittimo interesse perseguito dal titolare del trattamento o da un terzo. L'interesse del titolare del trattamento o del terzo può essere più ampio della finalità del trattamento e deve essere esistente e attuale al momento del trattamento stesso[6].

8. La base giuridica del legittimo interesse richiede, in secondo luogo, la necessità di trattare i dati personali per il perseguimento del legittimo interesse in questione. Per quanto riguarda quest'ultima condizione, a patto che il titolare del trattamento abbia un legittimo interesse come sopra indicato, non è evidente che la conservazione dei dati della carta di credito per facilitare acquisti futuri sia necessaria per perseguire tale legittimo interesse. Infatti, l'effettiva conclusione di un altro acquisto dipende dalla scelta del consumatore e non è determinata dalla possibilità di realizzarla «in un solo clic».

9. Infine, la terza condizione richiede l'esecuzione di un test di bilanciamento: il legittimo interesse del titolare del trattamento o del terzo deve essere bilanciato con gli interessi o i diritti e le libertà fondamentali dell'interessato, compresi i diritti dell'interessato alla protezione dei dati e alla vita privata. Il bilanciamento richiede che si tenga conto delle circostanze specifiche del trattamento[7]. Una componente essenziale del test di bilanciamento è l'impatto potenziale sui diritti e sulle libertà dell'interessato derivante dal trattamento[8]. Tale impatto può dipendere dalla natura dei dati, dalle modalità specifiche di trattamento e dall'accesso a tali dati da parte di terzi. Per quanto riguarda il criterio della natura dei dati, va osservato che i dati finanziari sono stati qualificati dal gruppo di lavoro «Articolo 29» come dati di natura altamente personale in quanto la loro violazione implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato[9]. Pertanto, nonostante l'obbligo del titolare del trattamento di attuare misure tecniche e organizzative per garantire un'adeguata sicurezza dei dati delle carte di credito ai sensi dell'articolo 5, paragrafo 1, lettera f), RGPD, e il fatto che tali dati possano essere conservati per altri scopi, il loro trattamento per facilitare ulteriori acquisti può comportare un rischio crescente di violazioni della sicurezza dei dati in questione, in quanto implica il trattamento in altri sistemi. Un altro elemento importante ai fini del bilanciamento da effettuare per valutare l'impatto del trattamento sugli interessati è costituito dalle ragionevoli aspettative degli interessati stessi in base al loro rapporto con il titolare del trattamento, al contesto e alla finalità della raccolta di dati personali[10]. Tuttavia, sembra di poter affermare che al momento dell'acquisto, pur fornendo i dati della carta di credito per il pagamento, l'interessato non preveda ragionevolmente che i dati della sua carta di credito siano conservati più a lungo

di quanto necessario per pagare i prodotti o i servizi che sta acquistando. Di conseguenza, è verisimile che i diritti e le libertà fondamentali della persona interessata prevalgano sugli interessi del titolare del trattamento in questo specifico contesto.

10. Le considerazioni che precedono portano a concludere che il consenso [articolo 6, paragrafo 1, lettera a), RGPD] sembra essere l'unica base giuridica idonea ad assicurare la liceità del trattamento sopra descritto. Infatti, al fine di gestire i rischi per la sicurezza, consentire all'interessato di mantenere il controllo sui propri dati e decidere attivamente in merito all'uso dei dati relativi al credito, è opportuno ottenere il consenso specifico dell'interessato prima di conservare i dati della sua carta di credito dopo un acquisto. Tale consenso consentirà al titolare del trattamento di dimostrare la volontà della persona di facilitare ulteriori acquisti attraverso il sito web o l'applicazione specifici, il che non è presumibile semplicemente per il fatto che quella persona ha concluso una o più operazioni isolate.
11. Il consenso non può essere presunto, ma deve essere libero, specifico, informato e inequivocabile[11]. Deve essere fornito mediante un'azione positiva inequivocabile e dovrebbe essere richiesto in modo semplice, ad esempio attraverso una casella di spunta, che non dovrebbe essere preselezionata[12], direttamente sul modulo utilizzato per la raccolta dei dati. Tale consenso specifico deve essere distinto dal consenso fornito per le condizioni di servizio o di vendita e non deve costituire una condizione per la realizzazione dell'operazione.
12. Ai sensi dell'articolo 7, paragrafo 3, RGPD, l'interessato ha il diritto di revocare in qualsiasi momento il proprio consenso alla conservazione dei dati della carta di credito al fine di facilitare ulteriori acquisti. La revoca deve essere libera, semplice e facile per l'interessato, allo stesso modo del consenso. Essa deve risultare nell'effettiva cancellazione, da parte del titolare del trattamento, dei dati della carta di credito conservati al solo scopo di facilitare ulteriori operazioni.

Per il comitato europeo per la protezione dei dati

La presidente

(Andrea Jelinek)

NOTE

[1] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI - Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679.

[2] Va osservato che le presenti Raccomandazioni non riguardano gli istituti di pagamento che operano nei negozi online, né le autorità pubbliche. Né tanto meno la conservazione dei dati delle carte di credito per qualsiasi altro scopo, ad esempio per adempiere un obbligo legale o per creare un pagamento ricorrente in caso di contratto a esecuzione continua o di abbonamento a un servizio a lungo termine (ad esempio un contratto che prevede la fornitura di un determinato prodotto ogni mese o l'abbonamento a un servizio di fornitura di musica o filmati in streaming).

[3] Cfr. altresì le Linee guida EDPB 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, in particolare pagina 10.

[4] Cfr. il parere del gruppo di lavoro «Articolo 29» sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, attualmente in fase di revisione da parte del comitato (cfr. il programma di lavoro dell'EDPB 2021/2022 adottato il 16 marzo 2021).

[5] Cfr. la sentenza della CGUE del 4 maggio 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde contro Rīgas pašvaldības SIA "Rīgas satiksme", causa C 13/16, ECLI:EU:C:2017:336, punto 28.

[6] Cfr. la sentenza della CGUE dell'11 dicembre 2019, TK contro Asociaţia de Proprietari bloc M5A-ScaraA, causa C 708/18, ECLI:EU:C:2019:1064, punto 44.

[7] Cfr. la sentenza della CGUE del 24 novembre 2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) contro Administración del Estado, cause C 468/10 e C 469/10, ECLI:EU:C:2011:777, punti 47 e 48; e la sentenza della CGUE del 19 ottobre 2016, Patrick Breyer contro Bundesrepublik Deutschland, causa C 582/14, ECLI:EU:C:2016:779, punto 62.

[8] Cfr. la sentenza della CGUE del 24 novembre 2011, citata, punto 44; e la sentenza della CGUE dell'11 dicembre 2019, citata, punto 56.

[9] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI - Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679.

[10] Cfr. il considerando 47 del RGPD.

[11] Cfr. le Linee guida 05/2020 sul consenso ai sensi del regolamento (UE) 2016/679.

[12] *Ibid*.

Decisione di esecuzione (UE) 2021/915 della Commissione

del 4 giugno 2021

relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) **(1)**, in particolare l'articolo 28, paragrafo 7,

visto il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE **(2)**, in particolare l'articolo 29, paragrafo 7,

considerando quanto segue:

(1) I concetti di titolare del trattamento e di responsabile del trattamento hanno un ruolo cruciale nell'applicazione del regolamento (UE) 2016/679 e del regolamento (UE) 2018/1725. Il titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Ai fini del regolamento (UE) 2018/1725, per titolare del trattamento si intende l'istituzione o l'organo dell'Unione, la direzione generale o qualunque altra entità organizzativa che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Quando le finalità e i mezzi di tale trattamento sono determinati da un atto specifico dell'Unione, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione. Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

(2) Al rapporto tra titolari del trattamento e responsabili del trattamento soggetti al regolamento (UE) 2016/679 e tra titolari del trattamento e responsabili del trattamento soggetti al regolamento (UE) 2018/1725 dovrebbe applicarsi lo stesso insieme di clausole contrattuali tipo. Questo perché, per assicurare un approccio coerente alla protezione dei dati personali in tutta l'Unione e la libera circolazione dei dati personali all'interno dell'Unione, le norme sulla protezione dei dati del regolamento (UE) 2016/679, applicabili al settore pubblico negli Stati membri, e le norme sulla protezione dei dati del regolamento (UE) 2018/1725, applicabili alle istituzioni, agli organi e agli organismi dell'Unione, sono state per quanto possibile allineate tra loro.

(3) Per garantire il rispetto delle prescrizioni dei regolamenti (UE) 2016/679 e (UE) 2018/1725, quando affida delle attività di trattamento a un responsabile del trattamento, il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in

atto misure tecniche e organizzative che soddisfino i requisiti dei regolamenti (UE) 2016/679 e (UE) 2018/1725, anche per la sicurezza del trattamento.

(4) I trattamenti da parte di un responsabile del trattamento devono essere disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli gli elementi elencati all'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 o all'articolo 29, paragrafi 3 e 4, del regolamento (UE) 2018/1725. Tale contratto o atto è stipulato in forma scritta, anche in formato elettronico.

(5) A norma dell'articolo 28, paragrafo 6, del regolamento (UE) 2016/679 e dell'articolo 29, paragrafo 6, del regolamento (UE) 2018/1725, il titolare del trattamento e il responsabile del trattamento possono scegliere di negoziare un contratto individuale contenente gli elementi obbligatori di cui, rispettivamente, all'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 o all'articolo 29, paragrafi 3 e 4, del regolamento (UE) 2018/1725, oppure di utilizzare, in tutto o in parte, le clausole contrattuali tipo adottate dalla Commissione in conformità dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725.

(6) Il titolare del trattamento e il responsabile del trattamento dovrebbero essere liberi di includere le clausole contrattuali tipo stabilite nella presente decisione in un contratto più ampio e di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo o pregiudichino i diritti o le libertà fondamentali degli interessati. L'utilizzo delle clausole contrattuali tipo lascia impregiudicato qualunque obbligo contrattuale del titolare del trattamento e/o del responsabile del trattamento di garantire il rispetto dei privilegi e delle immunità applicabili.

(7) Le clausole contrattuali tipo dovrebbero contenere norme sia sostanziali che procedurali. In linea con l'articolo 28, paragrafo 3, del regolamento (UE) 2016/679 e l'articolo 29, paragrafo 3, del regolamento (UE) 2018/1725, le clausole contrattuali tipo dovrebbero inoltre imporre al titolare del trattamento e al responsabile del trattamento di indicare la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali in questione e le categorie di interessati, nonché gli obblighi e i diritti del titolare del trattamento.

(8) In conformità dell'articolo 28, paragrafo 3, del regolamento (UE) 2016/679 e dell'articolo 29, paragrafo 3, del regolamento (UE) 2018/1725, il responsabile del trattamento deve informare immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione del titolare del trattamento violi il regolamento (UE) 2016/679 o il regolamento (UE) 2018/1725 o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

(9) Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività, si dovrebbero applicare i requisiti specifici di cui all'articolo 28, paragrafi 2 e 4, del regolamento (UE) 2016/679 o all'articolo 29, paragrafi 2 e 4, del regolamento (UE) 2018/1725.

In particolare, è necessaria un'autorizzazione preliminare scritta, specifica o generale. A prescindere dal carattere specifico o generale di tale autorizzazione, il primo responsabile del trattamento dovrebbe tenere un elenco aggiornato degli altri responsabili del trattamento.

(10) Per soddisfare i requisiti di cui all'articolo 46, paragrafo 1, del regolamento (UE) 2016/679, la Commissione ha adottato clausole contrattuali tipo in conformità dell'articolo 46, paragrafo 2, lettera c), dello stesso regolamento (UE) 2016/679. Tali clausole soddisfano anche i requisiti di cui all'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 per i trasferimenti di dati da titolari del trattamento soggetti al regolamento (UE) 2016/679 a responsabili del trattamento che non rientrano nell'ambito di applicazione territoriale di tale regolamento, o da responsabili del trattamento soggetti al regolamento (UE) 2016/679 a sub-responsabili del trattamento che non rientrano nell'ambito di applicazione territoriale di tale regolamento. Le presenti clausole contrattuali tipo non possono essere utilizzate come clausole contrattuali tipo ai fini del capo V del regolamento (UE) 2016/679.

(11) I terzi dovrebbero poter diventare parti delle clausole contrattuali tipo durante l'intero ciclo di vita del contratto.

(12) Il funzionamento delle clausole contrattuali tipo dovrebbe essere valutato nell'ambito della valutazione periodica del regolamento (UE) 2016/679 di cui all'articolo 97 di tale regolamento.

(13) Il garante europeo della protezione dei dati e il comitato europeo per la protezione dei dati sono stati consultati a norma dell'articolo 42, paragrafi 1 e 2, del regolamento (UE) 2018/1725 e hanno espresso un parere congiunto il 14 gennaio 2021 **(3)**, di cui si è tenuto conto nella preparazione della presente decisione.

(14) Le misure di cui alla presente decisione sono conformi al parere del comitato istituito a norma dell'articolo 93 del regolamento (UE) 2015/679 e dell'articolo 96, paragrafo 2, del regolamento (UE) 2015/1725,

HA ADOTTATO LA PRESENTE DECISIONE:

ARTICOLO 1

Le clausole contrattuali tipo figuranti in allegato soddisfano i requisiti per i contratti tra titolari del trattamento e responsabili del trattamento di cui all'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 e all'articolo 29, paragrafi 3 e 4, del regolamento (UE) 2018/1725.

ARTICOLO 2

Le clausole contrattuali tipo figuranti in allegato possono essere utilizzate nei contratti tra un titolare del trattamento e un responsabile del trattamento che tratta dati personali per conto del titolare del trattamento.

ARTICOLO 3

La Commissione valuta l'applicazione pratica delle clausole contrattuali tipo figuranti in allegato, sulla base di tutte le informazioni disponibili, nell'ambito della valutazione periodica prevista all'articolo 97 del regolamento (UE) 2016/679.

ARTICOLO 4

La presente decisione entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea.

Fatto a Bruxelles, il 4 giugno 2021

Per la Commissione
La presidente

Ursula VON DER LEYEN

(1) GU L 119 del 4.5.2016, pag. 1.

(2) GU L 295 del 21.11.2018, pag. 39.

(3) Parere congiunto 2/2021 dell'EDPB e del GEPD sulla decisione di esecuzione della Commissione europea relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento riguardo alle questioni di cui all'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 e all'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725.

ALLEGATO
Clausole contrattuali tipo

SEZIONE I

Clausola 1

Scopo e ambito di applicazione

a) Scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto [scegliere l'opzione pertinente: OPZIONE 1: dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)]/[OPZIONE 2: dell'articolo 29, paragrafi 3 e 4, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE].

b) I titolari del trattamento e i responsabili del trattamento di cui all'allegato I hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 e/o dell'articolo 29, paragrafi 3 e 4, del regolamento (UE) 2018/1725.

c) Le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.

d) Gli allegati da I a IV costituiscono parte integrante delle clausole.

e) Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725.

f) Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725.

Clausola 2

Invariabilità delle clausole

a) Le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati.

b) Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3

Interpretazione

a) Quando le presenti clausole utilizzano i termini definiti, rispettivamente, nel regolamento (UE) 2016/679 o nel regolamento (UE) 2018/1725, tali termini hanno lo stesso significato di cui al regolamento interessato.

b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725, rispettivamente.

c) Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679 / dal regolamento (UE) 2018/1725, o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4

Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

Clausola 5 — Facoltativa

Clausola di adesione successiva

a) Qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di responsabile del trattamento, compilando gli allegati e firmando l'allegato I.

b) Una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un responsabile del trat-tamento, conformemente alla sua designazione nell'allegato I.

c) L'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II
OBBLIGHI DELLE PARTI

Clausola 6

Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato II.

Clausola 7

Obblighi delle parti

7.1. Istruzioni

a) Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

b) Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo pare-re, le istruzioni del titolare del trattamento violino il regolamento (UE) 2016/679/ il regolamento (UE) 2018/1725 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei da-ti.

7.2. Limitazione delle finalità

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del titolare del trattamento.

7.3. Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II.

7.4. Sicurezza del trattamento

a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la

divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

b) Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati sensibili

Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili»), il responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari.

7.6. Documentazione e rispetto

a) Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole.

b) Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.

c) Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal regolamento (UE) 2016/679 e/o dal regolamento (UE) 2018/1725. Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

d) Il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.

e) Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Ricorso a sub-responsabili del trattamento

a) OPZIONE 1: AUTORIZZAZIONE PRELIMINARE SPECIFICA: Il responsabile del trattamento non può subcontrattare a un sub-responsabile del trattamento i trattamenti da effettuare per conto del titolare del trattamento conformemente alle presenti clausole senza la previa autorizzazione specifica scritta del titolare del trattamento. Il responsabile del trattamento presenta la richiesta di autorizzazione specifica almeno [SPECIFICARE IL PERIODO] prima di ricorrere al sub-responsabile del trattamento in questione, unitamente alle informazioni necessarie per consentire al titolare del trattamento di decidere in merito all'autorizzazione. L'elenco dei sub-responsabili del trattamento autorizzati dal titolare del trattamento figura nell'allegato IV. Le parti tengono aggiornato tale allegato.

   OPZIONE 2: AUTORIZZAZIONE SCRITTA GENERALE: Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. Il responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno [SPECIFICARE IL PERIODO], dando così al titolare del trattamento tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento in questione. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.

b) Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725.

c) Su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.

d) Il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.

e) Il responsabile del trattamento concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8. Trasferimenti internazionali

a) Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725.

b) Il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del regolamento (UE) 2016/679, il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del capo V del regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

Clausola 8

Assistenza al titolare del trattamento

a) Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

b) Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.

c) Oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8, lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:

   1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione

dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

2) l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

3) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;

4) gli obblighi di cui [OPZIONE 1] all'articolo 32 regolamento (UE) 2016/679/ [OPZIONE 2] agli articoli 33 e da 36 a 38 del regolamento (UE) 2018/1725.

d) Le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9

Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679 o degli articoli 34 e 35 del regolamento (UE) 2018/1725, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.1. Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:

a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso/(a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);

b) nell'ottenere le seguenti informazioni che, in conformità [OPZIONE 1] dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679/ [OPZIONE 2] dell'articolo 34, paragrafo 3, del regolamento (UE) 2018/1725, devono essere indicate nella notifica del titolare del trattamento e includere almeno:

1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

2) le probabili conseguenze della violazione dei dati personali;

3) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

c) nell'adempiere, in conformità [OPZIONE 1] dell'articolo 34 del regolamento (UE) 2016/679/ [OPZIONE 2] dell'articolo 35 del regolamento (UE) 2018/1725, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2. Violazione riguardante dati trattati dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);

b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;

c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma [OPZIONE 1] degli articoli 33 e 34 del regolamento (UE) 2016/679/[OPZIONE 2] degli articoli 34 e 35 del regolamento (UE) 2018/1725.

SEZIONE III
DISPOSIZIONI FINALI

Clausola 10

Inosservanza delle clausole e risoluzione

a) Fatte salve le disposizioni del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

b) Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:

   1) il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal tito-lare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristi-nato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;

   2) il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli ob-blighi che gli incombono a norma del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725;

   3) il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725.

ALLEGATO I

Elenco delle parti

Titolare/i del trattamento: [Identità e dati di contatto del/dei titolari del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]

1. Nome: ...
   Indirizzo: ...
   Nome, qualifica e dati di contatto del referente: ...
   Firma e data di adesione: ...
2. ...

Responsabile/i del trattamento [Identità e dati di contatto del/dei responsabili del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]

1. Nome: ...
   Indirizzo: ...
   Nome, qualifica e dati di contatto del referente: ...
   Firma e data di adesione: ...
2. ...

ALLEGATO II

Descrizione del trattamento

Categorie di interessati i cui dati personali sono trattati
…

Categorie di dati personali trattati
…

Dati sensibili trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari.
…

Natura del trattamento
…

Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento
…

Durata del trattamento
…

…

Per il trattamento da parte di (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento

ALLEGATO III

Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei dati

NOTA ESPLICATIVA:

Le misure tecniche e organizzative devono essere descritte in modo concreto e non genericamente.

Descrizione delle misure di sicurezza tecniche e organizzative messe in atto dal o dai responsabili del trattamento (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche. Esempi di possibili misure:

- misure di pseudonimizzazione e cifratura dei dati personali
- misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento
- misure di identificazione e autorizzazione dell'utente
- misure di protezione dei dati durante la trasmissione
- misure di protezione dei dati durante la conservazione
- misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati
- misure per garantire la registrazione degli eventi
- misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita
- misure di informatica interna e di gestione e governance della sicurezza informatica
- misure di certificazione/garanzia di processi e prodotti
- misure per garantire la minimizzazione dei dati
- misure per garantire la qualità dei dati
- misure per garantire la conservazione limitata dei dati
- misure per garantire la responsabilità
- misure per consentire la portabilità dei dati e garantire la cancellazione]

Per i trasferimenti a (sub-)responsabili del trattamento, descrivere anche le misure tecniche e organizzative specifiche che il (sub-)responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento.

Descrizione delle misure tecniche e organizzative specifiche che il responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento.

ALLEGATO IV

Elenco dei sub-responsabili del trattamento

NOTA ESPLICATIVA:

Il presente allegato deve essere compilato in caso di autorizzazione specifica di sub-responsabili del trattamento [clausola 7.7, lettera a), opzione 1].
Il titolare del trattamento ha autorizzato il ricorso ai seguenti sub-responsabili del trattamento:

1. Nome: ...
   Indirizzo: ...
   Nome, qualifica e dati di contatto del referente: ...
   Descrizione del trattamento (compresa una chiara delimitazione delle responsabilità qualora siano autorizzati più sub-responsabili del trattamento): ...
2. ...

Requisiti aggiuntivi di accreditamento degli organismi di certificazione

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e l'avv. Giuseppe Busia, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito il "Codice") come novellato dal d.lgs. 10 agosto 2018, n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679";

VISTO l'art. 42 del Regolamento, il quale prevede che i titolari e/o responsabili del trattamento possano aderire a meccanismi di certificazione della protezione dei dati nonché a sigilli e marchi di protezione dei dati (di seguito "meccanismi di certificazione") al fine di dimostrare la conformità al Regolamento dei trattamenti da loro effettuati (cfr. cons. 100 del Regolamento);

CONSIDERATO, in particolare, che l'adesione a un meccanismo di certificazione rilasciato a norma dell'art. 42, del Regolamento può costituire un elemento di responsabilizzazione (c.d. *accountability*), in quanto consente ai titolari e/o ai responsabili del trattamento che vi aderiscono di dimostrare la conformità dei medesimi trattamenti ad alcune disposizioni o principi del Regolamento, o al Regolamento nel suo insieme (cfr. cons. 77 e 81, nonché artt. 24, par. 3, 28, par. 5, 32, par. 3 e 42, par. 2 del Regolamento);

VISTO che nell'ambito dell'istituzione di meccanismi di certificazione è previsto che gli organismi di certificazione (di seguito "OdC"), che rilasciano certificazioni a norma dell'art. 42, par. 5 del Regolamento, debbano essere accreditati, in base a quanto stabilito dall'art. 43, par. 1 del Regolamento, dall'autorità di controllo competente o dall'organismo nazionale di accreditamento, o da entrambi;

CONSIDERATO che lo scopo dell'accreditamento consiste nel fornire una dichiarazione autorevole in ordine alla competenza di un determinato organismo a svolgere un'attività di certificazione (cfr. cons. 15 del Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, di seguito "Regolamento (CE) n. 765/2008") e che ciò consente di creare fiducia nel meccanismo stesso di certificazione;

VISTO che l'art. 2 *septiesdecies* del Codice attribuisce ad ACCREDIA, quale Ente unico nazionale di accreditamento istituito ai sensi del Regolamento (CE) n. 765/2008, le

funzioni di accreditamento degli OdC, ovvero di attestare che un determinato OdC sia qualificato a rilasciare le certificazioni ai sensi dell'art. 42, par. 5 del Regolamento in conformità a quanto previsto dall'art. 43, par. 1, lett. b) dello stesso;

CONSIDERATO che l'art. 43, par. 3 del Regolamento prevede che l'accreditamento degli OdC abbia luogo in base ai requisiti approvati dall'autorità di controllo competente ai sensi dell'art. 55 del Regolamento e che se l'accreditamento è effettuato dall'organismo nazionale di accreditamento ai sensi dell'art. 43, par. 1, lett. b) del Regolamento, i suddetti requisiti si aggiungono a quelli della norma tecnica EN-ISO/IEC 17065:2012 (di seguito "requisiti aggiuntivi") ;

CONSIDERATO che l'autorità di controllo competente presenta al Comitato europeo per la protezione di dati (di seguito "Comitato"), ai sensi del meccanismo di coerenza di cui all'art. 63 del Regolamento, uno schema di requisiti "aggiuntivi" per l'accreditamento di un OdC;

VISTE le Linee guida 4/2019 in materia di accreditamento degli organismi di certificazione a norma dell'art. 43 del Regolamento, adottate il 4 giugno 2019, dal Comitato all'esito della relativa consultazione pubblica e preso atto degli orientamenti ivi resi in ordine all'interpretazione e all'attuazione delle disposizioni di cui all'art. 43 del Regolamento, volti a individuare un sistema di regole coerente e armonizzato per l'accreditamento degli OdC;

VISTO in particolare il quadro organico di riferimento per i requisiti di accreditamento, delineato nell'Allegato 1 alle citate Linee guida, che integra la norma tecnica EN-ISO/IEC 17065:2012 e fornisce le indicazioni necessarie al fine di armonizzare l'elaborazione di tali requisiti aggiuntivi da parte delle autorità di controllo nazionali;

TENUTO CONTO che queste ultime hanno facoltà di individuare ulteriori requisiti aggiuntivi rispetto a quelli indicati nel predetto Allegato 1, purché gli stessi siano conformi al diritto nazionale (cfr. Allegato 1, Linee guida 4/2019, p. 14);

CONSIDERATO che l'art. 57, par. 1, lett. p) del Regolamento prevede che ciascuna autorità di controllo, sul proprio territorio, definisca e pubblichi i requisiti per l'accreditamento degli OdC, ai sensi dell'articolo 43 del Regolamento;

RILEVATO che, ai sensi dell'art. 55 del Regolamento in combinato disposto con l'Art. 2-*bis* del Codice, il Garante è l'autorità di controllo competente ad approvare i predetti requisiti di accreditamento "aggiuntivi" aventi validità nazionale, nell'esercizio del potere conferitole ai sensi dell'art. 57, par. 1, lett. p) del Regolamento;

VISTO lo schema di "Requisiti di accreditamento "aggiuntivi" con riguardo alla norma EN-ISO/IEC 17065:2012 e in conformità dell'articolo 43, paragrafi 1, lettera b) e 3, del Regolamento generale sulla protezione dei dati" approvato dal Garante in data 14 maggio 2020 e sottoposto in data 15 maggio 2020 al Comitato per il prescritto parere (art. 43, par. 3 e art. 64, par. 1, lett. c), del Regolamento);

VISTE le osservazioni rese dal Comitato nel parere adottato il 23 luglio 2020 (disponibile su https://edpb.europa.eu/) e comunicato al Garante dal Segretariato del CEPD il 25 luglio 2020;

RITENUTO, in ottemperanza a quanto previsto dall'art. 64, par. 7, del Regolamento, di aderire alle osservazioni contenute nel suddetto parere e di modificare lo schema di requisiti di accreditamento in conformità a tali osservazioni, dandone comunicazione alla presidente del Comitato;

RITENUTO quindi ai sensi dell'art. 57, par. 1, lett. p), del Regolamento di approvare i "Requisiti di accreditamento "aggiuntivi" con riguardo alla norma EN-ISO/IEC 17065:2012 e in conformità dell'articolo 43, paragrafi 1, lettera b) e 3, del Regolamento generale sulla protezione dei dati", opportunamente modificati alla luce del suddetto parere ed allegati al presente provvedimento del quale formano parte integrante;

VISTA la documentazione in atti:

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Pasquale Stanzione;

TUTTO CIÒ PREMESSO IL GARANTE:

a) ai sensi dell'art. 57, par. 1, lett. p) del Regolamento approva i "Requisiti di accreditamento "aggiuntivi" con riguardo alla norma EN-ISO/IEC 17065:2012 e in conformità dell'articolo 43, paragrafi 1, lettera b) e 3, del Regolamento generale sulla protezione dei dati", in allegato al presente provvedimento del quale formano parte integrante;
b) ai sensi dell'art. 64, par. 7 del Regolamento comunica alla presidente del Comitato il presente provvedimento, che recepisce i rilievi formulati nel parere richiamato in premessa;
c) invia copia della presente deliberazione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia ai fini della sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.

Roma, 29 luglio 2020

IL PRESIDENTE
f.to Stanzione

IL RELATORE
f.to Stanzione

IL SEGRETARIO GENERALE

f.to Busia

Allegato al provvedimento del Garante per la protezione dei dati personali n. 148 del 29 luglio 2020

Requisiti di accreditamento "aggiuntivi" dell'Autorità di controllo italiana con riguardo alla norma ISO/IEC 17065:2012 e in conformità dell'articolo 43, paragrafi 1, lettera b) e 3, del Regolamento Generale sulla Protezione dei Dati

I numeri delle sezioni utilizzati nel presente documento corrispondono a quelli utilizzati nella norma ISO/IEC 17065:2012.

I requisiti di accreditamento di seguito indicati sono corredati da alcune note esplicative, riportate in corsivo, che non hanno carattere vincolante, essendo volte a fornire indicazioni pratiche ed esempi che possono agevolare l'applicazione dei medesimi requisiti sia per la predisposizione della richiesta di accreditamento sia per il mantenimento dell'accreditamento stesso.

PREMESSA

Il decreto legislativo 30 giugno 2003, n. 196 (Codice per la protezione dei dati personali, di seguito "Codice"), come modificato dal decreto legislativo del 10 agosto 2018, n. 101, ha individuato in ACCREDIA, in quanto Ente unico nazionale di accreditamento, istituito ai sensi del Regolamento (CE) n. 765/2008, l'organismo nazionale deputato all'accreditamento degli organismi di certificazione secondo quanto previsto nell'articolo 43, par. 1, lettera b), del Regolamento 2016/679 (di seguito "Regolamento").

Fermo restando quanto previsto dall'art. 2-septiesdecies del Codice, il Garante per la protezione dei dati personali (nel seguito "Garante") e ACCREDIA hanno sottoscritto, in data 20 marzo 2019, una convenzione[1] volta a favorire lo scambio di informazioni in merito alle attività di accreditamento e certificazione previste dal Regolamento (artt. 42 e 43 del Regolamento), nonché a valorizzare le reciproche competenze.

1. AMBITO DI APPLICAZIONE

L'ambito di applicazione della norma ISO/IEC 17065:2012 è definito in conformità del Regolamento. Ulteriori informazioni sono riportate nelle linee guida relative all'accreditamento[2] e alla certificazione[3].

2. RIFERIMENTI NORMATIVI

Il Regolamento prevale sulla norma ISO/IEC 17065:2012. Qualora i requisiti aggiuntivi o il meccanismo di certificazione facciano riferimento ad altre norme ISO, esse dovranno essere interpretate in linea con i requisiti fissati nel Regolamento.

3. TERMINI E DEFINIZIONI

Nel contesto del presente documento si applicano i termini e le definizioni delle linee guida relative all'accreditamento e alla certificazione. Tali termini e definizioni prevalgono sulle definizioni dell'ISO a eccezione del termine "cliente". Tale termine viene utilizzato nel presente documento in senso conforme alla definizione di cui al paragrafo 3.1 della norma ISO/IEC 17065/2012 e, quindi, deve intendersi riferito tanto al "richiedente" (il soggetto che richiede la certificazione), quanto al "cliente" (il soggetto che ha ottenuto la certificazione).

4. REQUISITI GENERALI IN MATERIA DI ACCREDITAMENTO

4.1 ASPETTI GIURIDICI E CONTRATTUALI

4.1.1 RESPONSABILITÀ GIURIDICA

L'organismo di certificazione (nel seguito "OdC"), oltre a soddisfare il requisito di cui al punto 4.1.1 della norma ISO/IEC 17065:2012, è in grado di dimostrare (in qualsiasi momento) ad ACCREDIA di disporre di procedure aggiornate atte a comprovare la conformità alle responsabilità giuridiche fissate nei termini di accreditamento, compresi i requisiti aggiuntivi con riguardo all'applicazione del Regolamento.

L'OdC, nella richiesta di accreditamento, assume formalmente l'impegno di osservare ogni normativa applicabile allo svolgimento delle sue funzioni e, in particolare, le disposizioni rilevanti del Regolamento e del Codice.

L'OdC è in grado di fornire prova dell'esistenza di procedure e misure conformi al Regolamento finalizzate al controllo e alla gestione dei dati personali dell'organizzazione cliente nel quadro del processo di certificazione.

L'OdC informa ACCREDIA e il Garante, in caso di modifiche significative della propria situazione di fatto o di diritto.

L'OdC conferma ad ACCREDIA che non sono in corso procedimenti dinanzi al Garante tali da implicare il mancato soddisfacimento dei requisiti di accreditamento. ACCREDIA verifica tali informazioni con il Garante prima di avviare le attività relative al rilascio dell'accreditamento.

Nota esplicativa

Prova dell'esistenza di procedure e misure conformi al Regolamento finalizzate al controllo e alla gestione dei dati personali trattati dall'OdC può essere costituita dalla designazione di un RPD ai sensi dell'articolo 37 del Regolamento e dall'adozione di politiche e procedure per la protezione dei dati (data protection policy) ai sensi dell'articolo 24, paragrafo 2 del Regolamento.

Per modifiche significative della situazione di fatto o di diritto si intendono quelle modifiche ai requisiti sulla base dei quali l'OdC è stato accreditato che incidono sulla sua capacità di rilasciare certificazioni credibili e affidabili; con particolare riferimento ai requisiti relativi a responsabilità, imparzialità, capacità finanziaria, riservatezza, trasparenza, competenza, rapida ed efficace risposta ai reclami.

4.1.2 ACCORDO DI CERTIFICAZIONE

L'OdC dimostra, oltre al rispetto dei requisiti della norma ISO/IEC 17065:2012, che i propri accordi di certificazione:

1. impongano al cliente di ottemperare sempre sia ai requisiti generici di certificazione ai sensi del punto 4.1.2.2, lettera a), della norma ISO/IEC 17065:2012, sia ai criteri approvati dal Garante o dal Comitato europeo per la protezione dei dati (di seguito "Comitato") in conformità dell'articolo 43, paragrafo 2, lettera b) e dell'articolo 42, paragrafo 5 del Regolamento;

2. impongano al cliente di garantire nei confronti del Garante la piena trasparenza della procedura di certificazione, compresi gli aspetti contrattualmente riservati relativi alla conformità in materia di protezione dei dati a norma dell'articolo 42, paragrafo 7 e dell'articolo 58, paragrafo 1, lettera c) del Regolamento;
3. non limitino la responsabilità del cliente in merito alla conformità al Regolamento e lascino impregiudicati i compiti e i poteri del Garante in linea con l'articolo 42, paragrafo 5 del Regolamento;
4. impongano al cliente di fornire all'OdC tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione a norma dell'articolo 42, paragrafo 6 del Regolamento;
5. impongano al cliente di rispettare tutte le scadenze e le procedure applicabili. Nell'accordo di certificazione devono essere pattuite le scadenze e le procedure derivanti, a esempio, dal programma di certificazione o da altre normative che devono essere osservate e rispettate;
6. con riguardo al punto 4.1.2.2, lettera c), n. 1, della norma ISO/IEC 17065:2012, fissino regole sulla validità, sul rinnovo e sulla revoca in conformità dell'articolo 42, paragrafo 7 e dell'articolo 43, paragrafo 4 del Regolamento, inclusa la definizione di congrui intervalli di tempo per la rivalutazione o il riesame periodico in linea con l'articolo 42, paragrafo 7 del Regolamento;
7. consentano all'OdC di divulgare al Garante tutte le informazioni necessarie al rilascio della certificazione a norma dell'articolo 42, paragrafo 8 e dell'articolo 43, paragrafo 5 del Regolamento;
8. contemplino regole in merito alle precauzioni necessarie per le indagini sui reclami ai sensi del punto 4.1.2.2, lettera c), n. 2, e, inoltre, in conformità della lettera j), contengano indicazioni esplicite sulla struttura e sulla procedura per la gestione dei reclami in conformità dell'articolo 43, paragrafo 2, lettera d) del Regolamento;
9. oltre a soddisfare i requisiti di cui al punto 4.1.2.2 della norma ISO/IEC 17065:2012, disciplinino anche, se presenti, tutte le conseguenze della revoca o della sospensione dell'accreditamento dell'OdC che si ripercuotono sul cliente;
10. impongano al cliente di informare senza indebito ritardo l'OdC e il Garante, su richiesta, in caso di modifiche significative della propria situazione di fatto o di diritto o dei propri prodotti, processi e servizi oggetto della certificazione.

Nota esplicativa

Le informazioni che il cliente fornisce all'OdC riguardano anche gli eventuali procedimenti in corso dinanzi al Garante o le violazioni della disciplina in materia di protezione dei dati personali tali da implicare il mancato soddisfacimento dei criteri di certificazione.

Per modifiche significative della situazione di fatto o di diritto si tenga anche conto delle indicazioni contenute nella Nota 3 al requisito 4.1.2 della ISO 17065:2012.

Per modifiche significative dei propri prodotti, processi e servizi si intendono quelle tali da configurare una modifica dell'oggetto della certificazione, in quanto comportano integrazioni o variazioni significative dell'oggetto della certificazione ovvero della tipologia di un prodotto, dell'ambito di un processo o delle modalità di erogazione di un servizio [es. interfacce, trasferimenti ad altri sistemi e organizzazioni, protocolli, canali e/o piattaforme di erogazione, metodi per il trattamento, tecnologie utilizzate, logica degli algoritmi per le decisioni automatizzate, misure tecniche e organizzative, modifica del responsabile del trattamento,...].

4.1.3 UTILIZZO DI SIGILLI E MARCHI DI PROTEZIONE DEI DATI

I certificati, i marchi e i sigilli devono essere usati esclusivamente in conformità degli articoli 42 e 43 del Regolamento e delle linee guida relative all'accreditamento e alla certificazione.

4.2 GESTIONE DELL'IMPARZIALITÀ

ACCREDIA garantisce che, oltre a soddisfare il requisito di cui al punto 4.2 della norma ISO/IEC 17065:2012:

11. l'OdC sia conforme ai seguenti requisiti aggiuntivi:

- fornisca prova separata della propria indipendenza in linea con l'articolo 43, paragrafo 2, lettera a) del Regolamento, in particolare per quanto riguarda il finanziamentodell'organismo, nella misura in cui tale aspetto incida sulla garanzia della sua imparzialità;
- fornisca la prova di cui al punto precedente, su richiesta, al Garante, per quanto riguarda il finanziamentodell'OdC;
- i suoi compiti e le sue funzioni non diano adito a un conflitto di interessi in linea con l'articolo 43, paragrafo 2, lettera e) del Regolamento;

12. l'OdC non abbia alcun collegamento rilevante con il cliente che valuta.

Nota esplicativa

Per il concetto di imparzialità si tenga anche conto di quanto contenuto della Nota 2 del par. 3.2 della ISO 17021-1:2015.

L'OdC rappresenta una terza parte indipendente che non ha relazione con i soggetti che deve sottoporre a valutazione ai fini del rilascio della certificazione. La direzione (top management) e il personale dell'OdC responsabile della valutazione di conformità non devono aver ricoperto alcun ruolo nella progettazione, produzione, fornitura, installazione, acquisizione del prodotto, processo o servizio oggetto di valutazione, né esserne i proprietari, gli utenti o i manutentori, e non possono agire in qualità di rappresentanti autorizzati di soggetti che abbiano ricoperto o ricoprano i suddetti ruoli.

Imparzialità e indipendenza possono essere comprovate, a esempio, attraverso la seguente documentazione:

- *statuto e atto costitutivo dell'OdC;*
- *regole e procedure di composizione, nomina, modalità di remunerazione e durata del mandato dei componenti dell'OdC incaricati di assumere le decisioni attinenti alle attività di certificazione;*
- *documentazione comprovante i rapporti commerciali, finanziari, contrattuali o di altro genere che intercorrono tra l'OdC e il cliente.*

Riguardo il conflitto di interessi, quest'ultimo può sussistere, per esempio:

a) qualora l'OdC abbia una qualsiasi relazione economica con il cliente tale da incidere sul proprio fatturato o generare anche parzialmente condizionamenti di natura economica;

b) qualora l'OdC, o i suoi soci, abbiano quote o partecipazioni in società che offrono consulenza rispetto a prodotti, processi, servizi oggetto di certificazione;

c) qualora l'OdC svolga attività assimilabili alla consulenza non adeguatamente mitigate, quali a esempio:
   - *fornire personale che assume il ruolo di RPD (articolo 37 del Regolamento);*
   - *altre attività di valutazione della conformità, in presenza o meno di accreditamento;*
   - *altre attività quali, a esempio, la verifica dell'osservanza della normativa vigente, prove di penetrazione (penetration test), rilevamento delle intrusioni (intrusion detection).*

Per maggiori dettagli su imparzialità e conflitto di interessi si veda anche la Guida EA-2/20 Consultancy, and the Independence of Conformity Assessment Bodies[4].

4.3 RESPONSABILITÀ E FINANZIAMENTO

ACCREDIA verifica regolarmente che l'OdC, oltre a rispettare il requisito di cui al punto 4.3.1 della norma ISO/IEC 17065:2012, disponga di idonee misure (a esempio un'assicurazione o riserve finanziarie) tali da coprire le proprie responsabilità nelle aree geografiche in cui opera.

L'OdC, quale attestazione della piena osservanza, più in generale, degli obblighi di legge in materia, conferma di non essere oggetto di procedure concorsuali o fallimentari, di essere in regola con il versamento dei contributi pensionistici e assistenziali, di non essere oggetto di procedimenti coattivi di riscossione tributi e che i suoi rappresentanti legali non hanno riportato condanne definitive per reati colposi o dolosi collegati alle attività dell'OdC.

L'OdC dimostra anche l'osservanza dei requisiti di cui alla norma ISO/IEC 17021-1:2015, punto 5.3.2, ossia di aver valutato i rischi derivanti dalle attività di certificazione e di avere adottato, sulla base di tale pregressa valutazione, misure idonee a mitigare i rischi individuati. A tale fine, l'OdC mette a disposizione di ACCREDIA e del Garante, su richiesta, la documentazione pertinente.

Nota esplicativa

I rischi derivanti dalle attività di certificazione possono comprendere, ma non limitarsi:

- *agli obiettivi dell'audit:*
- *al campionamento utilizzato nel processo di audit;*
- *all'imparzialità reale e percepita;*
- *alle questioni relative a responsabilità e obblighi giuridici;*
- *all'organizzazione del cliente sottoposta ad audit e al suo ambiente operativo;*
- *all'impatto dell'audit sul cliente e le sue attività;*
- *alla salute e sicurezza dei gruppi di audit;*
- *alle dichiarazioni fuorvianti da parte del cliente;*
- *all'utilizzo di marchi.*

Misure idonee alla mitigazione dei rischi individuati possono comprendere la stipula di polizze assicurative sufficienti a coprire eventuali richieste di risarcimento, accantonamenti in bilancio, ecc... Nella definizione dei relativi importi, l'OdC dovrebbe tenere conto delle risultanze della valutazione del rischio.

L'analisi del rischio dovrebbe essere sottoposta a revisione periodica, almeno annuale, per identificare nuovi rischi o modifiche ai medesimi in riferimento alle attività e alle relazioni dell'OdC o del suo personale.

4.4 CONDIZIONI NON DISCRIMINATORIE

Non si formulano requisiti aggiuntivi rispetto al punto 4.4 della norma ISO/IEC 17065:2012.

4.5 RISERVATEZZA

Oltre a rispettare il requisito di cui al punto 4.5 della norma ISO/IEC 17065:2012, l'OdC è responsabile della gestione di tutte le informazioni raccolte o utilizzate durante le attività relative al rilascio della certificazione e, a tal fine, garantisce ai suoi clienti (attuali e potenziali) che il proprio personale, in modo particolare il personale dedicato alle attività di valutazione e di decisione, mantenga riservate tali informazioni, fermo restando il rispetto di eventuali obblighi di legge che prevedano diversamente.

4.6 INFORMAZIONI DISPONIBILI AL PUBBLICO

Oltre al rispetto del requisito di cui al punto 4.6 della norma ISO/IEC 17065:2012, ACCREDIA esige dall'OdC almeno che:

1. tutte le versioni (attuali e precedenti) dei criteri approvati utilizzati ai sensi dell'articolo 42, paragrafo 5 del Regolamento, così come tutte le procedure di certificazione, siano pubblicate e facilmente accessibili al pubblico, con indicazione generale del rispettivo periodo di validità;
2. le informazioni sulle procedure di gestione dei reclami e sui ricorsi siano rese pubbliche a norma dell'articolo 43, paragrafo 2, lettera d) del Regolamento.

5. REQUISITI STRUTTURALI

5.1 STRUTTURA ORGANIZZATIVA E ALTA DIREZIONE

Non si formulano requisiti aggiuntivi rispetto al punto 5.1 della norma ISO/IEC 17065:2012.

5.2 MECCANISMI DI SALVAGUARDIA DELL'IMPARZIALITÀ

Non si formulano requisiti aggiuntivi rispetto al punto 5.2 della norma ISO/IEC 17065:2012.

6. REQUISITI PER LE RISORSE UMANE

6.1 PERSONALE DELL'ORGANISMO DI CERTIFICAZIONE

ACCREDIA garantisce che il personale dell'OdC, oltre a rispettare i requisiti di cui alla sezione 6 della norma ISO/IEC 17065:2012:

1. abbia dimostrato competenze adeguate e costantemente aggiornate (insieme di conoscenze ed esperienze) riguardo alla protezione dei dati a norma dell'articolo 43, paragrafo 1 del Regolamento;
2. sia indipendente e costantemente competente riguardo all'oggetto della certificazione a norma dell'articolo 43, paragrafo 2, lettera a) del Regolamento, e non presenti alcun conflitto di interessi a norma dell'articolo 43, paragrafo 2, lettera e) del Regolamento;
3. si impegni a rispettare i criteri di cui all'articolo 42, paragrafo 5 e dell'articolo 43, paragrafo 2, lettera b) del Regolamento;
4. con riguardo al personale dell'OdC responsabile delle decisioni relative alle certificazioni (*decision maker*), soddisfi i seguenti requisiti di onorabilità:
   a) non trovarsi o non essersi trovato in una delle condizioni previste dall'art. 2382 del codice civile;
   b) non essere stato radiato da albi professionali per motivi disciplinari né per altri motivi;
   c) non aver riportato condanne per delitti non colposi o a pena detentiva per contravvenzioni, salvi gli effetti della riabilitazione;
   d) non essere o non essere stato sottoposto a misure di prevenzione o di sicurezza personali di carattere processual-penale;
5. disponga di conoscenze ed esperienze pertinenti e adeguate per quanto riguarda l'applicazione della legislazione in materia di protezione dei dati;
6. disponga di conoscenze ed esperienze pertinenti e adeguate per quanto riguarda le pertinenti misure tecniche e organizzative di protezione dei dati;
7. sia in grado di dimostrare di avere adeguata e aggiornata esperienza nei settori menzionati nei requisiti aggiuntivi di cui ai punti 6.1.1, 6.1.4 e 6.1.5, nello specifico:

per il *personale con competenze tecniche*:

- di avere ottenuto una qualifica in un pertinente settore di competenza tecnica pari ad almeno il livello 6 dell'EQF[5] o un titolo abilitante riconosciuto (p. es. Dipl. Ing.) per la pertinente professione regolamentata, oppure di disporre di significativa esperienza professionale nello stesso settore.
- Al *personale responsabile delle decisioni relative alla certificazione* è richiesta una significativa esperienza professionale nell'identificazione e nell'attuazione delle misure di protezione dei dati.
- Al *personale responsabile delle valutazioni* è richiesta un'esperienza professionale nell'ambito della protezione tecnica dei dati e conoscenze ed esperienze in materia di procedure comparabili (es. certificazioni/audit) e, se del caso, iscrizione al relativo albo professionale.

Il personale dovrà dimostrare di mantenere aggiornate le conoscenze specifiche del settore riguardo alle competenze tecniche e di audit mediante formazione permanente documentata.

per il *personale con competenze giuridiche*:

- studi giuridici in un'università dell'UE o riconosciuta da uno stato di durata pari ad almeno otto semestri, compresa una specializzazione post-laurea (LL.M) o titoli equivalenti, oppure significativa esperienza professionale.
- Il *personale responsabile delle decisioni relative alla certificazione* deve dimostrare una significativa esperienza professionale nell'ambito della disciplina della protezione dei dati e, se del caso, deve essere iscritto al relativo albo professionale.
- Il *personale responsabile delle valutazioni* deve dimostrare almeno due anni di esperienza professionale nell'ambito della disciplina della protezione dei dati, e conoscenze ed esperienze in materia di procedure comparabili (es. certificazioni/audit) e, se del caso, deve essere iscritto al relativo albo professionale.

Il personale dovrà dimostrare di mantenere aggiornate le conoscenze specifiche del settore riguardo alle competenze tecniche e di audit mediante formazione permanente documentata.

L'OdC definisce e illustra ad ACCREDIA quali requisiti di esperienza professionale siano adeguati in rapporto all'ambito dello schema di certificazione e all'oggetto della valutazione.

Nota esplicativa

*Si considera "adeguato" il livello di competenza necessario all'effettivo svolgimento delle funzioni dell'OdC in relazione allo schema di certificazione per il quale viene richiesto l'accreditamento, avuto riguardo in particolare alle specificità del/i settore/i a cui si applica lo schema, alla categoria dei dati trat*tati e alla complessità delle attività di trattamento, ai diversi interessi coinvolti, nonché ai rischi per gli interessati.

Si considera "pertinente" l'esperienza attinente all'ambito della certificazione.
Per il personale responsabile delle decisioni relative alla certificazione tali requisiti si intendono soddisfatti, per esempio, se il personale, con adeguata esperienza in ambito certificazioni, possiede una certificazione accreditata secondo la UNI 11697:2017 almeno di Specialista Privacy o è in possesso dei requisiti di conoscenza, abilità e competenza e di accesso ai profili professionali previsti da tale norma tecnica e riportati in Allegato 1.

Per il personale responsabile delle valutazioni (ossia i membri del gruppo di verifica) tali requisiti si intendono soddisfatti, per esempio, se il personale possiede una certificazione accreditata secondo la UNI 11697:2017 del profilo di Valutatore Privacy o è in possesso dei requisiti di conoscenza, abilità e competenza e di accesso al suddetto profilo professionale previsti da tale norma tecnica e riportati in Allegato 1.

6.2 RISORSE PER LA VALUTAZIONE

Non si formulano requisiti aggiuntivi rispetto al punto 6.2 della norma ISO/IEC 17065:2012.

7. REQUISITI DI PROCESSO

7.1 ASPETTI GENERALI

Oltre al rispetto del requisito di cui al punto 7.1 della norma ISO/IEC 17065:2012, ACCREDIA garantisce che:

1. nel presentare la domanda di accreditamento l'OdC soddisfi i presenti requisiti aggiuntivi stabiliti del Garante ai sensi dell'articolo 43, paragrafo 1, lettera b) del Regolamento, in modo tale che i loro compiti e obblighi non diano adito a conflitto di interessi a norma dell'articolo 43, paragrafo 2, lettera e) del Regolamento;
2. prima di cominciare a utilizzare in un nuovo Stato membro, attraverso una sede distaccata, un sigillo europeo di protezione dei dati precedentemente approvato, l'OdC informi le autorità di controllo interessate.

7.2 DOMANDA

Oltre a quanto previsto dal punto 7.2 della norma ISO/IEC 17065:2012, l'OdC garantisce che:

1. l'oggetto della certificazione (Oggetto della Valutazione, OdV) sia descritto in dettaglio nella domanda di certificazione compresi le interfacce e i flussi di dati ad altri sistemi e organizzazioni, i protocolli e le altre garanzie;
2. nella domanda sia specificata la eventuale contitolarità circa il trattamento oggetto di certificazione e/o l'eventuale ricorso a responsabili del trattamento e, qualora il cliente sia un contitolare e/o responsabile del trattamento, siano descritti i suoi compiti e le sue responsabilità, nonché riportati il/i perti-

nente/i contratto/i o altro atto giuridico volto a regolare i rapporti tra titolare e contitolare e/o responsabile del trattamento.

7.3 ESAME DELLA DOMANDA

Oltre a quanto previsto dal punto 7.3 della norma ISO/IEC 17065:2012, l'OdC garantisce che:

1. nell'accordo di certificazione siano stabiliti metodi di valutazione vincolanti con riguardo all'oggetto della valutazione (OdV);
2. la valutazione di cui al punto 7.3, lettera e) tenga conto in misura appropriata sia delle competenze tecniche sia di quelle giuridiche in materia di protezione dei dati e assicuri la presenza di entrambe;

7.4 VALUTAZIONE

Oltre a quanto previsto dal punto 7.4 della norma ISO/IEC 17065:2012, l'OdC garantisce che i propri processi di certificazione descrivano metodi di valutazione sufficienti a valutare la conformità del/i trattamento/i ai criteri di certificazione, tra cui a esempio, laddove applicabili:

1. un metodo per valutare la necessità e la proporzionalità del/i trattamento/i rispetto al loro scopo e agli interessati;
2. un metodo per valutare la copertura, la composizione e la valutazione di tutti i rischi presi in considerazione dal titolare del trattamento e dal responsabile del trattamento con riguardo alle conseguenze giuridiche a norma degli articoli 30, 32, 35 e 36 del Regolamento e alla definizione delle misure tecniche e organizzative a norma degli articoli 24, 25 e 32 del Regolamento, nella misura in cui i suddetti articoli si applicano all'oggetto della certificazione;
3. un metodo per valutare i mezzi di tutela incluse le garanzie e le procedure atte ad assicurare la protezione dei dati personali nell'ambito del/i trattamento/i collegato/i all'oggetto della certificazione nonché a dimostrare il rispetto dei requisiti giuridici definiti nei criteri; e
4. documentazione riguardante i metodi e le relative risultanze.

L'OdC garantisce che tali metodi di valutazione siano standardizzati e applicabili di regola. Ciò significa che metodi di valutazione comparabili sono utilizzati per oggetti di valutazione (OdV) comparabili. Qualsiasi deroga a tale procedura è motivata dall'OdC.

Oltre a quanto previsto dal punto 7.4.2 della norma ISO/IEC 17065:2012, è ammessa la possibilità di affidare l'esecuzione della valutazione a esperti esterni riconosciuti dall'OdC sulla base dei requisiti di cui al precedente punto 6.1.
Oltre a quanto previsto dal punto 7.4.5 della norma ISO/IEC 17065:2012, è prevista la possibilità che una certificazione preesistente, che copra parte dell'oggetto della certificazione, possa essere tenuta in considerazione ai fini della valutazione relativa rilascio di una certificazione di protezione dei dati ai sensi degli arti-

coli 42 e 43 del Regolamento. Tuttavia, la preesistente certificazione, o la relativa dichiarazione, non può considerarsi, di per sé, sostitutiva delle valutazioni (parziali) riguardanti la certificazione ai sensi del Regolamento, né della relazione di certificazione e l'OdC, comunque, verifica la conformità ai criteri di certificazione in relazione all'oggetto della certificazione. Pertanto, il rilascio della certificazione di protezione dei dati, in ogni caso, avviene sulla base di una relazione di valutazione completa o di informazioni tali da consentire una valutazione delle certificazioni esistenti e dei suoi risultati che comprenda anche un'analisi comparativa (gap analysis) a cura dell'OdC circa l'eventuale scostamento fra i criteri, i metodi di valutazione e quanto rileva nello specifico oggetto di certificazione.

Oltre a quanto previsto dal punto 7.4.6 della norma ISO/IEC 17065:2012, l'OdC specifica, tramite idonea documentazione, le modalità con cui sono fornite al cliente le informazioni obbligatorie a norma del punto 7.4.6 in merito alle eventuali non conformità riscontrate. Devono essere definite almeno le tipologie e le tempistiche di tali informazioni.

Oltre a quanto previsto dal punto 7.4.9 della norma ISO/IEC 17065:2012, la documentazione è resa pienamente accessibile al Garante, su richiesta. Il Garante si riserva, inoltre, la possibilità di far partecipare agli audit di certificazione proprio personale in qualità di osservatore.

Nota esplicativa

I mezzi di tutela comprendono tutti gli strumenti e le procedure idonei a conseguire l'applicazione della normativa in materia di protezione dei dati nello specifico contesto dello schema di certificazione, alla luce delle disposizioni del GDPR e di quelle nazionali pertinenti.

La documentazione di cui al requisito aggiuntivo del punto 7.4.6 può corrispondere allo schema di certificazione, ovvero, qualora l'OdC non sia il titolare dello schema, a un diverso documento relativo al processo di certificazione.

7.5 RIESAME

Oltre a quanto previsto dal punto 7.5 della norma ISO/IEC 17065:2012, sono richieste procedure per la concessione, il riesame periodico e la revoca delle rispettive certificazioni a norma dell'articolo 43, paragrafi 2 e 3 del Regolamento.

7.6 DECISIONE RELATIVA ALLA CERTIFICAZIONE

Oltre a quanto previsto dal punto 7.6.1 della norma ISO/IEC 17065:2012, l'OdC:

1. specifica nelle procedure in che modo garantisce la propria indipendenza e responsabilità rispetto alle singole decisioni di rilascio di certificazione;
2. verifica con il suo cliente, prima dell'adozione della decisione sulla certificazione, che questi non sia oggetto di eventuali procedimenti dinanzi al Garante tali da implicare il mancato soddisfacimento dei criteri di certificazione.

7.7 DOCUMENTAZIONE RIGUARDANTE LA CERTIFICAZIONE

Oltre a quanto previsto dal punto 7.7.1, lettera e), della norma ISO/IEC 17065:2012 e in conformità dell'articolo 42, paragrafo 7 del Regolamento il periodo di validità delle certificazioni non può essere superiore a tre anni.

Oltre a quanto previsto dal punto 7.7.1, lettera e), della norma ISO/IEC 17065:2012, è obbligatoriamente documentata anche la sorveglianza periodica prevista al successivo punto 7.9.

Oltre a quanto previsto dal punto 7.7.1, lettera f), della norma ISO/IEC 17065:2012, l'OdC denomina l'oggetto della certificazione all'interno della relativa documentazione (indicando la versione o altre caratteristiche analoghe, laddove applicabili).

7.8 ELENCO DEI PRODOTTI, PROCESSI E SERVIZI CERTIFICATI

Oltre a quanto previsto dal punto 7.8 della norma ISO/IEC 17065:2012, l'OdC:

1. conserva le informazioni riguardanti i prodotti, i processi e i servizi certificati in modo che siano disponibili sia al personale interno sia al pubblico. L'OdC fornisce al pubblico una sintesi della relazione di valutazione. Scopo di tale sintesi è contribuire a una maggiore trasparenza sull'oggetto della certificazione e sulle modalità della relativa valutazione. La sintesi illustrerà tra l'altro:
   (a) l'ambito della certificazione e una descrizione significativa dell'oggetto della certificazione (OdV),
   (b) i rispettivi criteri di certificazione (inclusa la versione o lo stato funzionale),
   (c) i metodi di valutazione e i test effettuati, nonché
   (d) i(l) risultato/i.
2. a norma dell'articolo 43, paragrafo 5 del Regolamento informa il Garante in merito ai motivi del rilascio o della revoca della certificazione.

7.9 SORVEGLIANZA

Oltre a quanto previsto dai punti 7.9.1, 7.9.2 e 7.9.3 della norma ISO/IEC 17065:2012 e in conformità dell'articolo 43, paragrafo 2, lettera c) del Regolamento, durante il periodo di sorveglianza l'OdC prevede misure di sorveglianza periodica, stabilite sulla base di una valutazione del rischio, al fine della verifica della sussistenza dei requisiti di mantenimento della certificazione.

Nota esplicativa

Le procedure di sorveglianza, anche in termini di strutture e risorse a ciò dedicate, devono essere trasparenti, appropriate allo schema di certificazione per cui si richiede l'accreditamento, efficaci e verificabili, nonché praticabili dal punto di vista operativo. Tali pro-

cedure possono prevedere la pubblicazione di relazioni riguardanti le verifiche effettuate, di rapporti periodici o sintetici sulle attività svolte dall'OdC e le complessive risultanze di tali attività.

7.10 MODIFICHE CHE INFLUENZANO LA CERTIFICAZIONE

Oltre a quanto previsto dai punti 7.10.1 e 7.10.2 della norma ISO/IEC 17065:2012, tra le modifiche che influenzano la certificazione di cui l'OdC tiene conto rientrano: le modifiche alla legislazione in materia di protezione dei dati, l'adozione di atti delegati della Commissione europea in conformità dell'articolo 43, paragrafi 8 e 9 del Regolamento, le decisioni e i documenti del Comitato, la giurisprudenza in materia di protezione dei dati, le modifiche relative allo stato dell'arte.
Le modifiche possono essere gestite con procedure che prevedano, a esempio, periodi transitori, processi di approvazione da parte del Garante, nuova valutazione dell'oggetto della certificazione, ove pertinente, e misure adeguate per la revoca della certificazione qualora il trattamento oggetto di certificazione non sia più conforme ai criteri aggiornati.

7.11 TERMINE, RIDUZIONE, SOSPENSIONE O REVOCA DELLA CERTIFICAZIONE

Oltre a quanto previsto dal punto 7.11.1 della norma ISO/IEC 17065:2012, l'OdC stabilisce procedure per informare senza indebito ritardo e per iscritto il Garante e ACCREDIA, se pertinente, in merito alle misure messe in atto e al mantenimento, alla riduzione, alla sospensione e alla revoca delle certificazioni anche a seguito di reclami o ricorsi trattati conformemente al punto 7.13.
In conformità dell'articolo 58, paragrafo 2, lettera h) del Regolamento, l'OdC è tenuto a rispettare le decisioni e le prescrizioni del Garante che gli ingiungano di revocare o non rilasciare la certificazione a un cliente se il Garante ritiene che i criteri per la certificazione non sono o non sono più soddisfatti.

7.12 REGISTRAZIONI

Oltre a quanto previsto dal punto 7.11.1 della norma ISO/IEC 17065:2012, l'OdC conserva tutta la documentazione in forma completa, comprensibile, aggiornata e verificabile per un periodo di 3 anni dalla scadenza della certificazione.

7.13 RECLAMI E RICORSI, ARTICOLO 43, PARAGRAFO 2, LETTERA D) DEL REGOLAMENTO

Fatto salvo il diritto degli interessati di presentare reclamo al Garante o ricorso all'autorità giudiziaria ai sensi degli artt. 77 e 79 del Regolamento e degli art. 140-bis ss. del Codice, l'OdC garantisce che un interessato ovvero un organismo, organizzazione o associazione rappresentativa o attiva nel settore della protezione dati personali, possa proporre reclamo.

La procedura di gestione dei reclami rispetta i principi di partecipazione, imparzialità e garanzia del contraddittorio. In particolare, tale procedura prevede che l'OdC informi il reclamante dello stato o dell'esito del reclamo entro tempi ragionevoli, tali da consentire un'analisi accurata di quanto lamentato.

Oltre a quanto previsto dal punto 7.13.1 della norma ISO/IEC 17065:2012, l'OdC definisce:

(a) i soggetti che possono presentare reclami e appelli,

(b) i soggetti dell'OdC che trattano tali reclami e appelli,

(c) le verifiche effettuate in tale contesto,

(d) le possibilità di consultazione delle parti interessate,

(e) le modalità con cui garantisce la separazione tra le attività di certificazione e la gestione di appelli e reclami.

Oltre a quanto previsto dal punto 7.13.2 della norma ISO/IEC 17065:2012, l'OdC definisce:

(a) come e a chi dovrà essere trasmessa la conferma della ricezione del reclamo o dell'appello,

(b) i termini entro i quali la stessa dovrà essere trasmessa,

(c) le successive procedure.

Nota esplicativa

Per "tempi ragionevoli" entro cui l'OdC informa il reclamante dello stato o dell'esito del reclamo si intendono, di regola, 3 mesi.

8. REQUISITI DEL SISTEMA DI GESTIONE

Un requisito generale del sistema di gestione in conformità della sezione 8 della norma ISO/IEC 17065:2012 è la necessità di documentare, valutare, controllare e monitorare in maniera indipendente l'attuazione, da parte dell'OdC accreditato, nell'ambito dell'applicazione del meccanismo di certificazione, di tutti i requisiti contenuti nelle precedenti sezioni.

Il principio fondamentale della gestione è la definizione di un sistema in base al quale gli obiettivi della stessa siano fissati in modo efficace ed efficiente (nello specifico l'attuazione dei servizi di certificazione, per mezzo di adeguate specifiche). Ciò presuppone la trasparenza e la verificabilità dell'attuazione dei requisiti di accreditamento da parte dell'OdC, nonché la conformità permanente agli stessi.

A tal fine il sistema di gestione deve specificare una metodologia per il soddisfacimento e la verifica continua di tali requisiti, in conformità alla disciplina di protezione dei dati.

Tali principi di gestione e la loro documentata attuazione sono trasparenti e sono divulgati dall'OdC accreditato nell'ambito della procedura di accreditamento a norma dell'articolo 58 del Regolamento, nonché, successivamente, su richiesta del Garante, durante eventuali indagini condotte a titolo di revisione in materia di protezione dei dati a norma dell'articolo 58, paragrafo 1, lettera b) del Regolamento, ovvero in sede di riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7, a norma dell'articolo 58, paragrafo 1, lettera c) del Regolamento.

In particolare l'OdC accreditato rende permanentemente e continuamente noto al pubblico quali certificazioni ha rilasciato e su quali basi (ovvero i meccanismi o gli schemi di certificazione), nonché la loro validità e il quadro di riferimento e le condizioni a cui è subordinata (cfr. considerando 100 del Regolamento).

Ai fini della trasparenza l'OdC:

a) tiene traccia dei principi alla base della valutazione di conformità (es. norme tecniche di riferimento, norme legislative o regolamentari, ecc.);
b) documenta le specifiche metodologie utilizzate nella definizione delle procedure di audit ai fini della valutazione di conformità;
c) documenta le attività ispettive e di audit e i miglioramenti apportati alle procedure definite, comprese le motivazioni e la tempistica di tali miglioramenti;
d) affida a soggetti terzi verifiche dei propri processi di valutazione della conformità;
e) documenta e monitora il rispetto degli obblighi di imparzialità;
f) motiva eventuali variazioni dei criteri di trasparenza documentale e di processo (in rapporto a singoli schemi di certificazione, alle modalità di verifica della conformità rispetto a tali schemi, ai requisiti minimi fissati nei contratti stipulati con i clienti).

8.1 REQUISITI GENERALI DEL SISTEMA DI GESTIONE

Non si formulano requisiti aggiuntivi rispetto al punto 8.1 della norma ISO/IEC 17065:2012.

8.2 DOCUMENTAZIONE DEL SISTEMA DI GESTIONE

Non si formulano requisiti aggiuntivi rispetto al punto 8.2 della norma ISO/IEC 17065:2012.

8.3 TENUTA SOTTO CONTROLLO DEI DOCUMENTI

Non si formulano requisiti aggiuntivi rispetto al punto 8.3 della norma ISO/IEC 17065:2012.

8.4 TENUTA SOTTO CONTROLLO DELLE REGISTRAZIONI

Non si formulano requisiti aggiuntivi rispetto al punto 8.4 della norma ISO/IEC 17065:2012.

8.5 RIESAME DELLA DIREZIONE

Non si formulano requisiti aggiuntivi rispetto al punto 8.5 della norma ISO/IEC 17065:2012.

8.6 AUDIT INTERNI

Non si formulano requisiti aggiuntivi rispetto al punto 8.6 della norma ISO/IEC 17065:2012.

8.7 AZIONI CORRETTIVE

Non si formulano requisiti aggiuntivi rispetto al punto 8.7 della norma ISO/IEC 17065:2012.

8.8 AZIONI PREVENTIVE

Non si formulano requisiti aggiuntivi rispetto al punto 8.8 della norma ISO/IEC 17065:2012.

9. ULTERIORI REQUISITI AGGIUNTIVI

9.1 AGGIORNAMENTO DEI METODI DI VALUTAZIONE

L'OdC istituisce procedure atte a guidare l'aggiornamento dei metodi di valutazione affinché possano essere applicati nel contesto della valutazione di cui al punto 7.4. L'aggiornamento ha luogo a seguito di modifiche al quadro giuridico, ai rischi pertinenti, allo stato dell'arte e ai costi di attuazione delle misure tecniche e organizzative.

Tali procedure consentono, con riguardo ai metodi di valutazione, l'individuazione e la documentazione di modifiche che interessano il quadro giuridico di riferimento, gli elementi del contratto stipulato fra il cliente e l'OdC, le fonti di rischio (nuove o emergenti, comprese vulnerabilità tecniche), lo stato dell'arte relativo ai trattamenti e alle misure tecniche e organizzative atte a garantire l'osservanza dei principi di protezione dei dati e la sicurezza dei trattamenti.

9.2 MANTENIMENTO DELLE COMPETENZE

L'OdC stabilisce procedure atte a garantire la formazione del proprio personale nell'ottica dell'aggiornamento delle loro competenze, tenuto conto degli sviluppi elencati al punto 9.1.

9.3 RESPONSABILITÀ E COMPETENZE

9.3.1 COMUNICAZIONE TRA L'ODC E I PROPRI CLIENTI

L'OdC prevede procedure finalizzate a mettere in atto meccanismi e strutture di comunicazione adeguate con il cliente. Tra queste rientrano:

1. il mantenimento della documentazione relativa ai compiti e alle responsabilità dell'OdC, al fine di
   a. rispondere a richieste di informazioni; o
   b. consentire i necessari contatti in caso di reclami relativi a una certificazione;
2. il mantenimento di una procedura di gestione delle domande di certificazione, al fine di:
   a. fornire informazioni sullo stato e l'esito di una domanda;
   b. consentire le valutazioni del Garante in merito a riscontri e decisioni della medesima Autorità.

9.3.2 DOCUMENTAZIONE DELLE ATTIVITÀ DI VALUTAZIONE

Non si formulano requisiti aggiuntivi.

9.3.3 GESTIONE DEI RECLAMI

L'OdC definisce, quale parte integrante del sistema di gestione, un meccanismo di gestione dei reclami e appelli che attui in particolare i requisiti di cui al punto 4.1.2.2, lettere c) e j), al punto 4.6, lettera d), e al punto 7.13 della norma ISO/IEC 17065:2012.

9.3.4 GESTIONE DELLE RIDUZIONI, SOSPENSIONI E REVOCHE

L'OdC integra nel proprio sistema di gestione le procedure in caso di riduzione, sospensione o revoca dell'accreditamento e riguardanti in particolare la relativa notifica ai propri clienti.

ALLEGATO 1 - APPENDICE B UNI 11697:2017 - REQUISITI PER L'ACCESSO AI PROFILI PROFESSIONALI

I percorsi di accesso, non alternativi tra loro, prevedono:
a) Apprendimento formale (titolo di studio);
b) Apprendimento non formale (formazione specifica);
c) Apprendimento informale (esperienza lavorativa).

Il prospetto B.1 prevede i requisiti di accesso ai vari profili professionali.

prospetto B.1 - Requisiti di accesso per profili professionali.

LIVELLO	TITOLO DI STUDIO	FORMAZIONE SPECIFICA	ESPERIENZA LAVORATIVA	EQUIPOLLENZA
Responsabile protezione dati	Laurea che includa discipline almeno in parte afferenti alle conoscenze del professionista privacy, legali o tecnico/ informatiche[6].	Corso di almeno 80 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[7].	Minimo 6 anni di esperienza lavorativa legata alla privacy di cui almeno 4 anni in incarichi di livello manageriale[8].	Se in possesso di laurea magistrale l'esperienza lavorativa si riduce a 4 anni di cui 3 in incarichi di livello manageriale. Se in possesso di diploma di scuola media superiore minimo 8 anni di esperienza lavorativa di privacy di cui almeno 5 anni in incarichi di livello manageriale.
Manager privacy	Laurea che includa discipline almeno in parte afferenti alle conoscenze del professionista privacy, legali o tecnico/ informatiche[6].	Corso di almeno 60 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[7].	Minimo 6 anni di esperienza lavorativa legata alla privacy di cui almeno 3 anni in incarichi di livello manageriale[8].	Se in possesso di laurea magistrale l'esperienza lavorativa si riduce a 4 anni di cui 2 in incarichi di livello manageriale. Se in possesso di diploma di scuola media superiore minimo 8 anni di esperienza lavorativa di privacy di cui almeno 4 anni in incarichi di livello manageriale.
Specialista privacy	Diploma di scuola media superiore.	Corso di almeno 24 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[7].	Minimo 4 anni di esperienza lavorativa legata alla privacy.	Se in possesso di laurea l'esperienza lavorativa si riduce a 2 anni.
Valutatore privacy	Diploma di scuola media superiore.	Corso di almeno 40 ore con attestazione finale avente per argomento la gestione della privacy e della sicurezza delle informazioni[7].	Minimo 6 anni di esperienza lavorativa continuativa legata alla privacy di cui almeno 3 anni in incarichi di audit.	Se in possesso di laurea l'esperienza lavorativa si riduce a 4 anni di cui 2 in incarichi di audit. Se in possesso di Laurea Magistrale minimo 3 anni di esperienza lavorativa di cui 2 in incarichi di audit.

NOTE

[1] https://www.gpdp.it (doc. web 9099622).

[2] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) - Version 3.0 (4 Giugno 2019).

[3] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - Version 3.0 (4 Giugno 2019).

[4] https://european-accreditation.org/wp-content/uploads/2020/04/EA-2-20_Consultancy_rev00_April-2020.pdf

[5] Cfr. lo strumento di confronto dei quadri delle qualifiche, disponibile all'indirizzo https://ec.europa.eu/ploteus/en/compare?.

[6] un laureato con laurea non afferente alle conoscenze del professionista privacy, legali o tecnico / informatiche è da considerarsi equiparato a un diplomato di scuola media superiore.

[7] è ammissibile la riduzione delle ore di formazione richieste fino a un massimo del 10% (30% per il Valutatore Privacy) in caso di possesso di certificazioni professionali riconosciute come attinenti alle conoscenze richieste al professionista privacy in questione.

[8] gli incarichi di livello manageriale possono includere anche attività rilevante svolta nell'ambito di attività di consulenza o di prestazione d'opera condotta nell'ambito dell'esecuzione di ingaggi professionali.

Requisiti di accreditamento degli organismi di monitoraggio dei codici di condotta

Registro dei provvedimenti
n. 98 del 10 giugno 2020

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il dott. Antonello Soro, presidente, la dott.ssa Augusta Iannini, vicepresidente, la prof.ssa Licia Califano, la dott.ssa Giovanna Bianchi Clerici, componenti e il dott. Giuseppe Busia, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito il "Codice") come novellato dal d.lgs. 10 agosto 2018, n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679";

VISTO l'art. 40 del Regolamento che prevede che le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possano elaborare (modificare o prorogare) codici di condotta destinati a contribuire alla corretta applicazione del Regolamento in specifici settori di attività e in funzione delle particolari esigenze delle micro, piccole e medie imprese, e che tali codici devono essere approvati dall'autorità di controllo competente;

VISTO il considerando 98 del Regolamento che prevede che tali codici possono calibrare gli obblighi del titolare del trattamento e del responsabile del trattamento, tenuto conto dei potenziali rischi del trattamento per i diritti e le libertà degli interessati;

VISTE le "Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del Regolamento (UE) 2016/679" adottate dal Comitato europeo per la protezione di dati (di seguito "Comitato") il 4 giugno 2019, all'esito della consultazione pubblica;

CONSIDERATO in particolare che l'adesione ad un codice di condotta può essere utilizzata come elemento di responsabilizzazione (c.d. *accountability*), in quanto consente di dimostrare la conformità dei trattamenti di dati, posti in essere dai titolari e/o dai responsabili del trattamento che vi aderiscano, ad alcune disposizioni o principi del Regolamento, o al Regolamento nel suo insieme (cfr. cons. 77 e artt. 24, par. 3, e 28, par. 5, e 32, par. 3 del Regolamento);

CONSIDERATO che l'art. 41, par. 1, del Regolamento prevede che, fatti salvi i compiti e i poteri dell'autorità di controllo competente, la verifica dell'osservanza delle disposizioni di un codice di condotta, ai sensi dell'articolo 40 del Regolamento, è effettuata da un Organismo di monitoraggio (di seguito "Odm") in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento rilasciato a tal fine dalla medesima autorità, con la sola eccezione del trattamento effettuato da autorità pubbliche e da organismi pubblici per il quale non è necessaria l'istituzione di un Odm (art. 41, par. 6 del Regolamento);

CONSIDERATO che l'art. 41, par. 3, del Regolamento prevede che la predetta autorità di controllo presenta al Comitato uno schema di requisiti per l'accreditamento dell'Odm, ai sensi del meccanismo di coerenza di cui all'art. 63 del Regolamento;

CONSIDERATO che l'art. 57, par. 1, lett. p) del Regolamento prevede, in particolare, che ciascuna autorità di controllo, sul proprio territorio, definisce e pubblica i requisiti per l'accreditamento dell'Odm, ai sensi dell'art. 41;

RILEVATO che, ai sensi del combinato disposto di cui agli artt. 55 del Regolamento e 2-*ter* del Codice, il Garante è l'autorità di controllo competente ad approvare i presenti requisiti per l'accreditamento dell'Odm, nell'esercizio del potere conferitole ai sensi dell'art. 57, par. 1, lett. p, del Regolamento;

CONSIDERATO che il Regolamento e le Linee guida del Comitato sopra citate, fissano un quadro organico di riferimento per la definizione dei requisiti che l'Odm deve soddisfare per ottenere l'accreditamento;

RILEVATO che il Garante incoraggia lo sviluppo di codici di condotta per le micro, piccole e medie imprese al fine di promuovere un'attuazione effettiva del Regolamento, aumentare la certezza del diritto per titolari e responsabili del trattamento e rafforzare la fiducia degli interessati in ordine alla correttezza dei trattamenti di dati che li riguardano;

RILEVATO, in questo contesto, che l'obbligo di affidare il monitoraggio dei codici di condotta a un Odm accreditato non dovrebbe costituire un ostacolo allo sviluppo di tali strumenti e che, quindi, va riconosciuto un certo margine di flessibilità ai promotori dei codici di condotta nell'applicazione dei requisiti di accreditamento fissati dal Garante al fine di definire il modello di Odm più adeguato a controllarne l'osservanza, fermo restando il rispetto di quanto previsto dal Regolamento, dalle Linee guida e dai pertinenti pareri del Comitato;

RILEVATO altresì che il Garante nella procedura di accreditamento, volta a verificare che l'Odm soddisfi i predetti requisiti, tiene in considerazione le specificità dei trattamenti di dati personali afferenti al/i settore/i a cui si applica il codice di condotta e, in particolare, la natura e la dimensione del settore, la tipologia e il numero (anche atteso) di soggetti aderenti, la peculiarità e la complessità delle operazioni di trattamento oggetto del codice, nonché i rischi per gli interessati;

VISTO lo schema di requisiti per l'accreditamento dell'Odm approvato dal Garante in data 30 gennaio 2020 e sottoposto in data 31 gennaio 2020 al Comitato per il prescritto parere (art. 41 par. 3 e art. 64 par. 1 lett. c), del Regolamento);

VISTE le osservazioni rese dal Comitato nel parere adottato il 25 maggio 2020 e notificato al Garante il 28 maggio 2020 (disponibile su https://edpb.europa.eu/);

RITENUTO, in ottemperanza a quanto previsto dall'art. 64, par. 7, del Regolamento, di aderire alle osservazioni contenute nel suddetto parere e di modificare lo schema di requisiti per l'accreditamento in conformità a tali osservazioni, dandone comunicazione alla presidente del Comitato;

RITENUTO quindi ai sensi dell'art. 57, par.1, lett. p), del Regolamento di approvare i requisiti per l'accreditamento dell'Odm, opportunamente modificati alla luce del suddetto parere ed allegati al presente provvedimento del quale formano parte integrante;

VISTA la documentazione in atti:

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE la dott.ssa Giovanna Bianchi Clerici;

TUTTO CIÒ PREMESSO IL GARANTE:

a) ai sensi dell'art. 57, par. 1, lett. p), del Regolamento approva i requisiti per l'accreditamento dell'Odm riportati in allegato al presente provvedimento del quale formano parte integrante;
b) ai sensi dell'art. 64, par. 7 del Regolamento comunica alla presidente del Comitato il presente provvedimento, che recepisce i rilievi formulati nel parere richiamato in premessa;
c) invia copia della presente deliberazione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia ai fini della sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.

Roma, 10 giugno 2020

IL PRESIDENTE

f.to Soro

IL RELATORE
f.to Bianchi Clerici

IL SEGRETARIO GENERALE
f.to Busia

All.: n. 1

Requisiti per l'accreditamento degli organismi di monitoraggio dei codici di condotta

1. Procedura di accreditamento.

L'Odm di cui all'art. 41 del Regolamento (Ue) 2016/679 (di seguito "Regolamento") ottiene l'accreditamento se comprova il possesso dei requisiti di seguito indicati sulla base di una richiesta inviata al Garante per la protezione dei dati personali. La richiesta deve essere presentata in lingua italiana e corredata da ogni documentazione utile a comprovare il possesso di tali requisiti.

L'accreditamento è rilasciato dal Garante per un periodo massimo di 5 anni, ferma restando la possibilità per i soggetti titolari del codice di condotta di prevedere nel medesimo codice che il mandato dell'Odm abbia una durata inferiore.

Fatti salvi i compiti dell'Autorità connessi alla verifica, in qualunque momento, del rispetto da parte dell'Odm dei requisiti di accreditamento e dello svolgimento delle sue funzioni di monitoraggio in conformità al Regolamento, l'Autorità si riserva di avviare una revisione dell'accreditamento prima della sua scadenza qualora venga a conoscenza, anche a seguito degli esiti di attività ispettive, di elementi o fattori di rischio sopravvenuti che compromettano il rispetto da parte dell'Odm dei predetti requisiti ovvero dei suoi obblighi di monitoraggio oppure la conformità al Regolamento delle misure da questi adottate.

L'Odm manterrà pertanto l'accreditamento per tutta la durata per cui viene rilasciato a meno che, all'esito della revisione condotta dal Garante, l'Autorità non accerti che l'Odm non soddisfi più i requisiti per l'accreditamento o che questi non sia in grado di adempiere ai suoi obblighi di monitoraggio oppure che le misure da esso adottate violino il Regolamento.

Al fine di ottenere il rinnovo dell'accreditamento la relativa richiesta potrà essere inviata al Garante fino a tre mesi prima della scadenza del termine.

I presenti requisiti di accreditamento si applicano all'Odm che lo richiede, sia nel caso in cui si tratti di organismo interno sia nel caso in cui si tratti di organismo esterno al soggetto titolare del codice di condotta per il quale si richiede l'accreditamento (di seguito "Odm interno" o "Odm esterno")[1], a meno che non sia espressamente specificato che un determinato requisito è richiesto soltanto per una tipologia di Odm.

Poiché nell'applicazione di tali requisiti l'Autorità tiene in adeguata considerazione le specificità del/i settore/i a cui si applica il codice di condotta, affinché un Odm, accreditato per il monitoraggio di un determinato codice, possa svolgere compiti di controllo nei riguardi di un altro codice di condotta, sarà necessario avanzare al Garante una diversa richiesta di accreditamento.

[1] L'Odm non può essere costituito all'interno di un soggetto aderente al codice di condotta.

I requisiti di accreditamento di seguito indicati sono corredati da alcune note esplicative, riportate in corsivo, che non hanno carattere vincolante, essendo volte a fornire indicazioni pratiche ed esempi che possono agevolare l'applicazione dei medesimi requisiti sia per la predisposizione della richiesta di accreditamento sia per il mantenimento dell'accreditamento stesso.

2. Richiesta di accreditamento

La richiesta di accreditamento deve essere redatta in lingua italiana e deve contenere le seguenti informazioni:

- i dati identificativi del richiedente o, in caso di società, associazioni, fondazioni o altri enti, i dati identificativi del rappresentante legale e delle persone eventualmente preposte all'adozione delle decisioni relative alle attività di monitoraggio aventi rilevanza esterna;
- il codice fiscale/la partita IVA e, se del caso, con riferimento alle società registrate, il numero del registro delle imprese;
- la residenza del richiedente, o in caso di società, associazioni, fondazioni o altri enti, la sede legale che deve essere in ogni caso all'interno dello Spazio Economico Europeo;
- l'eventuale censimento all'interno dell'Indice nazionale dei domicili digitali delle imprese e dei professionisti (INI-PEC www.inipec.gov.it - art. 6-bis Codice Amministrazione Digitale - D. Lgs. n. 82/2005) o nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs. n. 82/2005);
- nel caso di società, associazioni, fondazioni o altri enti, lo statuto e l'atto costitutivo;
- il recapito prescelto per le comunicazioni relative alla domanda di accreditamento;
- l'indicazione della tipologia di Odm (ossia, interno od esterno);
- l'indicazione del codice di condotta per il quale è richiesto l'accreditamento;
- l'ambito nazionale o transnazionale di applicazione del codice di condotta.

La richiesta di accreditamento può essere inviata per posta o recapitata a mano al seguente indirizzo: Garante per la protezione dei dati personali, Piazza Venezia, 11 – 00187 ROMA oppure inviata in via telematica alla casella di posta elettronica: odm.accreditamento@gpdp.it.

Nella richiesta di accreditamento, l'Odm assume formalmente l'impegno di osservare ogni normativa applicabile allo svolgimento delle sue funzioni e, in particolare, le disposizioni rilevanti del Regolamento e del d. lgs. 30 giugno 2003 n. 196 recante il Codice in materia di protezione dei dati personali (di seguito "Codice").

Il soggetto che effettua la richiesta di accreditamento mediante la sottoscrizione e l'invio della stessa si assume la responsabilità, anche ai sensi dell'art. 168 del Codice, della veridicità di quanto dichiarato.

Alla richiesta di accreditamento deve, altresì, essere allegata ogni documentazione utile idonea a comprovare il possesso dei requisiti di accreditamento di seguito individuati.

3. Indipendenza e imparzialità

L'Odm deve dimostrare di poter assolvere ai propri compiti di controllo con piena indipendenza e imparzialità.

In particolare, devono essere predisposte specifiche regole e procedure formali per la costituzione, il funzionamento e la durata del mandato dell'Odm che assicurino che questo possa svolgere le proprie funzioni di controllo senza subire influenze, interferenze o condizionamenti di alcun tipo da parte del soggetto titolare del codice di condotta, degli aderenti o comunque dei soggetti eventualmente riconducibili al settore (professionale**,** industriale o altro) a cui il codice si applica.

Per ottenere l'accreditamento, il possesso, in capo all'Odm, dell'indipendenza e imparzialità necessarie per adempiere ai propri obblighi di controllo deve essere comprovato in relazione ai seguenti profili: a) forma giuridica e procedure decisionali; b) autonomia finanziaria; c) autonomia organizzativa; d) responsabilizzazione.

3.a) Forma giuridica e procedure decisionali

Le modalità di costituzione dell'Odm e di composizione del suo personale con poteri decisionali, le procedure di adozione e applicazione delle decisioni, le regole di funzionamento e la durata del mandato dell'Odm devono garantire che questi assolva ai suoi obblighi di controllo con piena indipendenza e imparzialità. In particolare, l'Odm deve dimostrare di non essere soggetto, in via diretta o indiretta, ad alcuna forma di controllo, direzione o vigilanza da parte del soggetto titolare del codice di condotta, dei soggetti aderenti o eventualmente riconducibili al settore (professionale, industriale o altro) a cui il codice si applica. Inoltre, l'Odm deve dimostrare di poter condurre le proprie attività di controllo senza subire alcuna forma di pressione esterna, di interferenza o condizionamento diretti o indiretti. L'Odm fornisce informazioni su eventuali legami di natura giuridica o economica con il soggetto titolare del codice di condotta e i soggetti aderenti, fornendo prova del fatto che tali legami non ne compromettono l'indipendenza né l'imparzialità.

Nel caso di un Odm interno, devono essere previste misure aggiuntive e specifiche tali da garantire che i rapporti con il soggetto titolare del codice di condotta non ne compromettano l'indipendenza e l'imparzialità né l'effettiva operatività dei suoi compiti di controllo.

Nel caso di un Odm esterno, va comprovato che questi non fornisca al soggetto titolare del codice di condotta, ai soggetti aderenti al codice o eventualmente riconducibili al settore (professionale, industriale o altro) a cui il codice si applica, alcun prodotto o servizio che possa in qualche modo compromettere la sua indipendenza e imparzialità ovvero l'effettiva operatività dei suoi compiti di controllo.

Nota esplicativa:
Ciò può essere comprovato, ad esempio, attraverso la seguente documentazione:

- *statuto e atto costitutivo dell'Odm e del soggetto titolare del codice di condotta;*
- *regole e procedure di selezione, nomina, modalità di remunerazione e durata del mandato dei componenti dell'Odm incaricati di assumere le decisioni attinenti alle attività di controllo;*
- *documentazione comprovante i rapporti commerciali, finanziari, contrattuali o di altro genere che intercorrono tra l'Odm, il soggetto titolare del codice di condotta e gli aderenti al codice nonché le idonee misure adottate allo scopo di ridurre al minimo eventuali rischi per l'indipendenza e l'imparzialità dell'Odm suddetto.*

3.b) Autonomia finanziaria

L'Odm deve dimostrare di disporre delle risorse finanziarie necessarie per l'effettivo adempimento dei suoi compiti nonché per far fronte alle sue responsabilità. Inoltre, l'Odm deve dimostrare che le regole e/o le modalità di finanziamento garantiscono la sostenibilità e la continuità delle attività di monitoraggio, in particolare qualora una o più fonti di tale finanziamento vengano a mancare successivamente, per esempio, in caso di ritiro o di esclusione di uno degli aderenti al codice di condotta, ove l'Odm sia finanziato attraverso le quote versate dagli aderenti stessi.

Nel valutare le proprie risorse finanziarie, l'Odm tiene conto del numero, delle dimensioni e della complessità organizzativa degli aderenti al codice di condotta, della natura e degli ambiti delle rispettive attività come definite dal codice e dei rischi connessi ai trattamenti cui il codice si applica.

L'Odm deve essere in grado di gestire le proprie risorse finanziarie in modo autonomo e indipendente senza alcuna forma di interferenza, condizionamento o controllo da parte del soggetto titolare del codice di condotta, degli aderenti allo stesso o comunque dei soggetti eventualmente riconducibili al settore (professionale, industriale o altro) a cui il codice si applica.

L'Odm deve dimostrare che le sue modalità di finanziamento sono approntate in modo tale da non pregiudicare l'indipendenza e l'imparzialità delle sue funzioni di controllo, nonché che siano oggetto di debita rendicontazione.

3.c) Autonomia organizzativa

L'Odm deve dimostrare di disporre di risorse umane, tecniche e logistiche adeguate per l'effettivo adempimento dei suoi obblighi di controllo, avuto riguardo in particolare alla specificità del/i settore/i a cui si applica il codice di condotta, tra cui, la natura e la dimensione del settore, la tipologia e il numero (anche atteso) dei soggetti aderenti, la delicatezza e la complessità dei trattamenti di dati oggetto del codice, i rischi per gli interessati. Tali risorse devono consentire all'Odm di svolgere le proprie funzioni di monitoraggio con piena indipendenza e imparzialità e senza subire alcuna forma di interferenza, condizionamento o sanzione, a causa dell'assolvimento delle stesse, ad opera del soggetto titolare del codice, dei soggetti aderenti o eventualmente riconducibili al settore (professionale, industriale o altro) a cui il codice si applica.

Nel caso di un Odm interno, quest'ultimo deve dimostrare che la sua struttura organizzativa sia configurata in modo tale da assicurare la sua indipendenza e imparzialità, nonché l'effettiva operatività delle sue funzioni di controllo.

Nota esplicativa:
Ciò può essere comprovato tramite la predisposizione di specifici modelli organizzativi e gestionali, di processi operativi che assicurino, ad esempio, la separazione organizzativa, gestionale e funzionale dell'Odm dal soggetto titolare del codice di condotta, nonché la confidenzialità delle informazioni trattate (per esempio: gestione amministrativa separata delle retribuzioni, sistemi contabili con distinti centri di imputazione di responsabilità, barriere informative e ogni altra misura atta a garantire la separazione delle funzioni gestionali e operative fra Odm e soggetto titolare del codice di condotta).

L'Odm deve dimostrare di disporre di personale qualificato, anche fornito da altro organismo indipendente dal soggetto titolare del codice, dai soggetti aderenti o eventualmente riconducibili al settore (professionale**,** industriale o altro) a cui il codice si applica. Tale personale, in ogni caso, deve essere soggetto alla direzione e alla vigilanza esclusiva dello stesso Odm e vincolato a specifici obblighi di confidenzialità nello svolgimento del suo operato.

Nota esplicativa:
Ad esempio, l'Odm può avvalersi di personale reclutato da un ente esterno indipendente che fornisce servizi di ricerca, formazione e selezione di risorse umane.

Qualora l'Odm si avvalga di collaboratori e fornitori esterni di servizi, appositamente delegati, per lo svolgimento di specifiche attività di controllo - ad eccezione di quelle che comportano l'esercizio di poteri decisionali, che non possono essere delegate ad alcuno - devono essere approntate cautele atte a garantire che tali soggetti siano individuati tra coloro che forniscono sufficienti garanzie di competenza e affidabilità, con particolare riferimento alla materia oggetto del codice di condotta. Tali cautele devono assicurare, altresì, che i medesimi requisiti di indipendenza, assenza di conflitto di interessi, rispetto della disciplina rilevante in materia di protezione dei dati personali, adeguatezza delle risorse, confidenzialità e competenza siano soddisfatti anche dai collaboratori e fornitori esterni di servizi appositamente delegati. Inoltre, le misure suddette devono garantire che l'Odm eserciti un controllo efficace sui servizi forniti da collaboratori e fornitori esterni. Infine, l'Odm deve dimostrare che i medesimi obblighi gravanti sullo stesso siano imposti in capo a detti collaboratori e fornitori esterni, restando inteso che l'Odm mantiene la responsabilità delle decisioni connesse alle attività di controllo e risponde in caso di inadempimento dei predetti obblighi da parte dei collaboratori e fornitori esterni.

Nota esplicativa:
Ciò può essere comprovato, ad esempio, tramite:

- *documentate procedure e regole organizzative per la selezione e l'utilizzo di collaboratori e fornitori esterni di servizi che definiscono le condizioni alle quali si possa ricorrere a tali soggetti, il processo autorizzativo e le modalità di controllo del loro operato;*
- *documentate procedure e regole organizzative atte a garantire la competenza e l'affidabilità di collaboratori e fornitori esterni di servizi;*
- *contratti o altri atti giuridici che individuino le rispettive responsabilità, ivi comprese quelle relative alla riservatezza e alla confidenzialità dei dati e delle altre informazioni trattate.*

3.d) Responsabilizzazione

L'Odm deve dimostrare di essere responsabile per le sue decisioni e azioni, ad esempio, definendo una serie di misure volte a documentare i processi decisionali, vigilare sul rispetto delle procedure interne di funzionamento e rendicontare le attività di controllo, in modo da garantire indipendenza e imparzialità.

Nota esplicativa:
Ciò può essere comprovato, ad esempio, tramite la descrizione delle procedure di lavoro, la redazione di relazioni di gestione e l'adozione di politiche di formazione del personale volte a renderlo edotto delle misure adottate.

Qualsiasi decisione assunta dall'Odm nell'ambito delle sue funzioni di controllo non deve essere soggetta all'approvazione di nessun altro ente, associazione o organizzazione, ivi inclusi il soggetto titolare del codice di condotta, gli aderenti allo stesso o i soggetti eventualmente riconducibili al settore (professionale, industriale o altro) a cui il codice si applica.

3.e) Onorabilità

I componenti dell'Odm incaricati di assumere le decisioni attinenti alle attività di controllo garantiscono i seguenti requisiti di onorabilità:

- non trovarsi in una delle condizioni previste dall'art. 2382 del codice civile;
- non essere stati radiati da albi professionali per motivi disciplinari né per altri motivi;
- non aver riportato condanne per delitti non colposi o a pena detentiva per contravvenzioni, salvi gli effetti della riabilitazione;
- non essere stati sottoposti a misure di prevenzione o di sicurezza personali.

Il possesso dei predetti requisiti di onorabilità nel caso di società, associazioni, fondazioni ed altri enti (persone giuridiche) devono essere riferiti al rappresentante legale e alle altre persone eventualmente preposte all'adozione delle decisioni relative alle attività di monitoraggio aventi rilevanza esterna.

4. Conflitto di interessi

L'Odm deve disporre di procedure documentate atte a prevenire, individuare, valutare, mitigare o rimuovere il rischio di eventuali conflitti di interesse per l'intera durata del suo mandato, avuto riguardo, in particolare, alle specificità del/i settore/i a cui si applica il codice di condotta. In particolare, tali procedure devono garantire che i singoli componenti dell'Odm con poteri decisionali e l'Odm nel suo complesso si astengano da qualunque azione incompatibile con le funzioni e gli obblighi di quest'ultimo e che non esercitino alcuna attività, remunerata o meno, con essi incompatibili. I componenti dell'Odm devono impegnarsi a rispettare tali procedure e a segnalare qualsiasi situazione che possa creare eventuali conflitti di interessi.

Nota esplicativa:
Ad esempio, può insorgere un conflitto di interessi nel caso in cui il personale dell'Odm con poteri decisionali abbia lavorato in precedenza per il soggetto titolare del codice o per uno degli aderenti oppure sia stato coinvolto nei lavori di redazione del codice di condotta. In casi del genere devono essere fornite all'Autorità garanzie idonee a mitigare sufficientemente il rischio di un eventuale conflitto di interessi.

La procedura di gestione dei conflitti di interesse può prevedere, ad esempio, che il personale dell'Odm con poteri decisionali sia tenuto a dichiarare per iscritto ogni potenziale conflitto di interessi o rischio per la propria indipendenza.

L'Odm deve predisporre misure atte ad assicurare che questi non solleciti o accetti istruzioni da alcuno, in particolare nella formazione, assunzione e applicazione delle decisioni attinenti all'assolvimento dei propri compiti di controllo.

L'Odm deve predisporre misure atte a evitare che lo stesso possa essere rimosso, sanzionato o penalizzato, direttamente o indirettamente, a causa dell'adempimento dei suoi compiti dai soggetti titolari del codice di condotta, dagli aderenti o dai soggetti in qualche modo riconducibili al settore (professionale**,** industriale o altro) a cui il codice si applica.

Nota esplicativa:
Ad esempio, l'assenza di conflitto di interessi può essere dimostrata attraverso elementi di valutazione desunti dalle procedure di selezione dei componenti dell'Odm con poteri decisionali, dalle relative modalità di remunerazione, dalla sottoscrizione di codici etici e dalle regole disciplinanti le condizioni per il rinnovo del loro incarico alla scadenza.

5. Competenza

L'Odm deve dimostrare di possedere un adeguato livello di competenza per il corretto ed efficiente svolgimento dei propri compiti di controllo in relazione allo specifico codice di condotta per il cui monitoraggio si richiede l'accreditamento.

In particolare, l'Odm deve dimostrare che i componenti che assumono le decisioni attinenti alle funzioni di monitoraggio, ivi compresi eventuali sostituti, posseggano, singolarmente o nel loro insieme:

- un'approfondita conoscenza ed esperienza (di tipo giuridico e informatico) in materia di protezione dei dati personali;
- un'approfondita conoscenza ed esperienza nel settore specifico o nelle specifiche attività di trattamento a cui si applica il codice di condotta;
- un'approfondita conoscenza ed esperienza nello svolgimento di compiti di vigilanza e controllo (ad esempio nel settore dell'audit o del controllo di qualità).

L'Odm deve dimostrare che il livello di conoscenza ed esperienza posseduto nei campi sopraindicati sia adeguato all'effettivo assolvimento dei suoi obblighi di controllo in relazione al codice di condotta per il quale viene richiesto l'accreditamento, avuto riguardo, in particolare, alle specificità del/i settore/i a cui si applica il codice, alla categoria dei dati trattati e alla complessità delle attività di trattamento, ai diversi interessi coinvolti, alla tipologia e al numero (anche atteso) di soggetti aderenti, nonché ai rischi per gli interessati.

L'Odm deve dimostrare altresì di possedere gli specifici requisiti di competenza definiti nel codice di condotta.

L'Odm deve garantire che la competenza posseduta sia oggetto di aggiornamento periodico in relazione all'evolversi della disciplina applicabile e della tecnologia utilizzata nel settore di riferimento del codice di condotta.

Nota esplicativa:
Requisiti di competenza più dettagliati sono fissati dal codice di condotta e sono considerati parte dell'accreditamento.

Si considera "adeguato" il livello di competenza necessario all'effettivo svolgimento delle funzioni di controllo assegnate all'Odm in relazione al codice di condotta per il quale viene richiesto l'accreditamento, avuto riguardo, in particolare, alle specificità del/i settore/i a

cui si applica il codice, alla categoria dei dati trattati e alla complessità delle attività di trattamento, ai diversi interessi coinvolti, alla tipologia e al numero (anche atteso) di soggetti aderenti nonché ai rischi per gli interessati.

Tali requisiti possono essere comprovati tramite il conseguimento di corsi di formazione professionale, diplomi di laurea, titoli di specializzazione o perfezionamento o master di durata almeno annuale, dottorati di ricerca, ovvero dal possesso di qualifiche ed esperienze professionali debitamente documentate o, ancora, da pubblicazioni a carattere scientifico o da ogni altro titolo comprovante qualificate esperienze professionali, di studio o di ricerca.

6. Procedure e strutture istituite per il monitoraggio del codice di condotta

L'Odm deve dimostrare di disporre di procedure idonee a valutare l'ammissibilità dei titolari e dei responsabili del trattamento ad aderire e ad applicare il codice di condotta, controllare l'osservanza delle sue disposizioni da parte di questi ultimi e riesaminare periodicamente il funzionamento del codice. Tali procedure devono essere approntate avendo riguardo a: la categoria dei dati trattati, la complessità delle attività di trattamento e i rischi derivanti per gli interessati, nonché la tipologia e il numero (anche atteso) dei soggetti aderenti al codice, l'ambito geografico in cui questo si applica, i reclami ricevuti e le violazioni eventualmente accertate.

La predetta procedura deve garantire che le richieste di adesione al codice di condotta da parte di titolari e responsabili del trattamento, se pervenute successivamente alla sua entrata in vigore del codice, siano esaminate entro termini ragionevoli.

L'Odm deve dimostrare che siffatta procedura preveda:

- la programmazione delle verifiche (iniziali, *ad hoc* e periodiche) durante un periodo di tempo definito e sulla base di criteri preventivamente individuati**,** quali la tipologia e il numero di aderenti al codice di condotta, l'ambito geografico, i reclami ricevuti, le violazioni accertate, ecc.;

- la conduzione delle verifiche sulla base di una metodologia definita, con particolare riferimento, al tipo di verifica da utilizzare (autovalutazione, *audit*, ispezioni, con o senza preavviso, in loco o in remoto, questionari, relazioni periodiche, ecc.), ai criteri oggetto di verifica e alle modalità di documentazione e gestione dei relativi risultati;

- la valutazione dei risultati delle verifiche che, nel rispetto dei principi di partecipazione, imparzialità e garanzia del contradditorio, consenta di identificare, istruire e gestire eventuali violazioni del codice di condotta da parte degli aderenti e di adottare entro termini ragionevoli, opportune misure correttive, anche sanzionatorie, volte a porre rimedio a tali violazioni e a prevenire il loro ripetersi, sulla base di quanto previsto dal codice di condotta in caso di violazione delle sue regole;

-che i soggetti aderenti al codice di condotta prestino la massima collaborazione ai fini del proficuo svolgimento di tali attività di controllo.

L'Odm è responsabile per la gestione di tutte le informazioni raccolte o utilizzate durante le procedure di controllo e, a tal fine, garantisce che il proprio personale mantenga riservate tali informazioni, fermo restando il rispetto di eventuali obblighi di legge che prevedano diversamente.

Nota esplicativa:
I requisiti sopra indicati sono volti a dimostrare che le procedure di monitoraggio proposte, anche in termini di strutture e risorse a ciò dedicate, siano trasparenti, appropriate al controllo del codice di condotta per cui si richiede l'accreditamento, nonché praticabili dal punto di vista operativo, efficaci e verificabili. Tali procedure possono prevedere la pubblicazione di relazioni riguardanti le verifiche effettuate o di rapporti periodici o sintetici sulle attività svolte dall'Odm e le complessive risultanze di tali attività.

7. Gestione trasparente dei reclami

L'Odm deve dimostrare di avere a disposizione un meccanismo che gli permetta di gestire in modo trasparente e imparziale i reclami aventi ad oggetto le violazioni del codice di condotta da parte degli aderenti o il modo in cui il codice di condotta è stato o è attuato da questi ultimi.

Fatto salvo il diritto degli interessati di presentare reclamo al Garante o ricorso all'autorità giudiziaria ai sensi degli artt. 77 e 79 del Regolamento e degli art. 140-bis e ss. del Codice, siffatto meccanismo deve garantire che un interessato ovvero un organismo, organizzazione o associazione rappresentativa o attiva nel settore della protezione dei dati personali, possa proporre reclamo all'Odm, inviando apposita istanza che contenga una breve descrizione dei fatti e del pregiudizio lamentato.

A tal fine, l'Odm deve dimostrare di aver messo in atto un adeguato quadro di procedure e strutture per la ricezione, l'istruttoria e la definizione dei reclami secondo quanto stabilito nel dettaglio nello stesso codice. Tali procedure devono essere trasparenti, intellegibili e facilmente accessibili a chiunque, nonché supportate da risorse appropriate in modo da garantire un'efficace gestione dei reclami.

La procedura di gestione dei reclami deve prevedere le modalità per la proposizione del reclamo nonché stabilire le modalità di definizione dello stesso, nel rispetto dei principi di partecipazione, imparzialità e garanzia del contradditorio. In particolare, tale procedura deve prevedere che l'Odm informi il reclamante dello stato e dell'esito del reclamo entro tempi ragionevoli, tali da consentire un'analisi accurata di quanto lamentato.

Fermo restando il rispetto dei predetti principi e garanzie, l'Odm deve dimostrare di poter adottare una o più misure correttive - anche sanzionatorie - come individuate nel codice di condotta, in caso di violazioni delle sue regole da parte degli aderenti, volte a porre rimedio a tali violazioni e a prevenire il loro ripetersi. Tali misure, a seconda della gravità della violazione riscontrata, devono poter includere la sospensione o l'esclusione dal codice di condotta del titolare/responsabile aderente al codice.

L'Odm deve dimostrare di aver approntato una procedura per informare senza indebito ritardo l'Autorità delle misure adottate e dei motivi della loro adozione nel caso di violazioni che comportino la sospensione o l'esclusione del titolare/responsabile aderente al codice.

L'Odm deve istituire e tenere costantemente aggiornato un registro di tutti i reclami e le azioni correttive, anche sanzionatorie, adottate a cui l'Autorità può accedere in qualsiasi momento.

L'Odm deve rendere pubblicamente accessibili le decisioni adottate all'esito della definizione dei reclami, previo oscuramento dei dati personali eventualmente presenti (in quanto riferiti a persone fisiche) anche attraverso informazioni di sintesi relative alle medesime decisioni, secondo quanto stabilito dalla procedura di gestione dei reclami e avuto riguardo alla gravità delle violazioni riscontrate e delle conseguenti misure impartite al titolare/responsabile aderente al codice.

Tali informazioni di sintesi devono, in ogni caso, comprendere i dati relativi a tutte le violazioni riscontrate che comportino la sospensione o l'esclusione dal codice e l'indicazione dei destinatari di tali misure nonché, a titolo esemplificativo e non esaustivo, informazioni riguardanti il numero e il tipo di reclami ricevuti, il tipo di violazioni riscontrate e le misure correttive impartite.

Nota esplicativa:

Un meccanismo di gestione dei reclami trasparente, imparziale e facilmente accessibile agli interessati è un elemento essenziale ai fini del monitoraggio del codice di condotta.

8. Comunicazioni all'Autorità di controllo

L'Odm deve dimostrare di aver approntato una procedura efficace per informare senza indebito ritardo l'Autorità dell'adozione delle misure più gravi adottate nei confronti del titolare/responsabile aderente al codice - quali la sospensione o l'esclusione dal medesimo codice - dei motivi della loro adozione e, in particolare, delle violazioni riscontrate, nonché delle azioni poste in essere dal titolare/responsabile sospeso o escluso dal codice per ottemperare a siffatte misure. Siffatta procedura deve consentire, altresì, all'Odm di informare senza indebito ritardo l'Autorità in caso di eventuale revoca di tali misure e delle motivazioni sottostanti.

La medesima procedura deve consentire all'Odm di fornire all'Autorità, su base annuale, un resoconto riassuntivo dei controlli effettuati, delle procedure di reclamo definite e delle misure eventualmente adottate nei confronti dei titolari/responsabili aderenti al codice.

In presenza di sopravvenute modifiche sostanziali ai requisiti, sulla base dei quali è stato rilasciato l'accreditamento, l'Odm dovrà senza indebito ritardo informarne l'Autorità.

Ogni modifica sostanziale sopravvenuta comporta la necessità di chiedere un nuovo accreditamento all'Autorità.

In particolare, per modifiche sostanziali sopravvenute si intendono quelle modifiche ai requisiti sulla base dei quali è stato rilasciato l'accreditamento che incidono sulla capacità dell'Odm di adempiere ai sui obblighi di monitoraggio in modo indipendente ed efficace, con le competenze adeguate e in assenza di conflitti d'interesse.

9. Meccanismi di riesame

L'Odm deve dimostrare di poter contribuire al riesame del funzionamento del codice di condotta tramite documentate procedure, in conformità a quanto stabilito nel medesimo codice e richiesto dal soggetto titolare del codice, al fine di garantire che quest'ultimo rimanga attuale e continui a contribuire alla corretta applicazione della disciplina sulla protezione dei dati personali.

In particolare, tali procedure assicurano che l'Odm fornisca periodicamente al soggetto titolare del codice di condotta - o a ogni altra associazione, organismo o ente previsto dal medesimo codice - informazioni significative sul suo funzionamento specie quelle che evidenziano la necessità di apportare modifiche o proroghe allo stesso.

L'Odm garantisce che le predette informazioni sul funzionamento del codice di condotta siano memorizzate e rese disponibili all'Autorità, ove richiesto.

Nota esplicativa:
Gli organismi di controllo svolgono un ruolo chiave nel contribuire alla revisione del codice di condotta in conformità alle procedure di revisione indicate nel medesimo codice. Ad esempio, si dovrebbero prevedere meccanismi di riesame per adeguare il codice di condotta all'evolversi della disciplina applicabile o qualora gli sviluppi tecnologici possano incidere sul trattamento dei dati personali da parte degli aderenti o sulle previsioni del medesimo codice. All'esito di tali procedure, il soggetto titolare del codice può proporre modifiche o proroghe al codice da sottoporre all'Autorità ai sensi dell'art. 40, par. 5 e ss., del Regolamento. A titolo esemplificativo e non esaustivo, si considerano significative le seguenti informazioni riguardanti il funzionamento del codice: quelle relative a nuovi soggetti aderenti, a eventuali sospensioni ed esclusioni dei membri del codice, alle violazioni riscontrate, ai reclami gestiti e, in generale, alle risultanze delle attività di controllo poste in essere dall'Odm.

10. Status giuridico

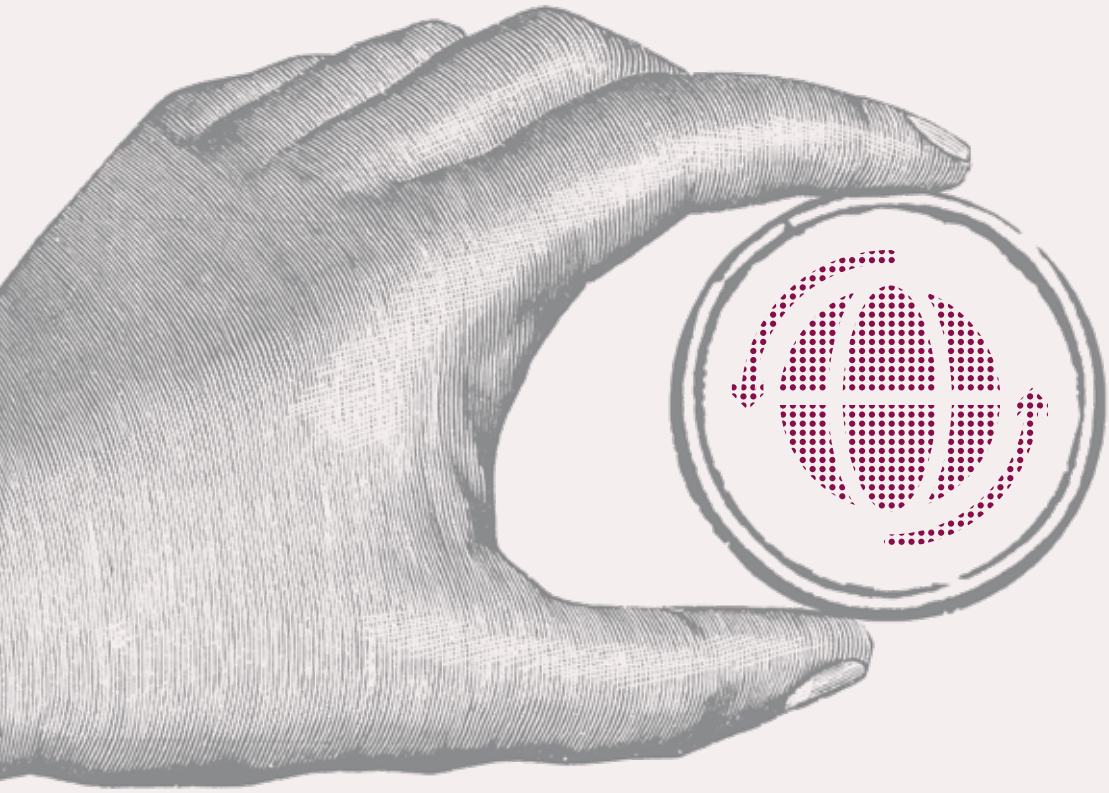
L'Odm deve dimostrare di essere stabilito all'interno del SEE.

Fermi restando i compiti e i poteri dell'Autorità secondo quanto previsto dal Regolamento e dal Codice in materia di protezione dei dati personali, l'Odm (interno o esterno) deve dimostrare di avere uno *status* giuridico tale da poter adempiere effettivamente ai suoi obblighi di controllo e far fronte alle connesse responsabilità.

Le modalità di costituzione dell'Odm e di composizione del suo personale con poteri decisionali, le procedure decisionali, le regole di funzionamento e la durata del mandato nonché le risorse di cui dispone devono garantire che l'Odm assolva ai suoi obblighi di controllo e possa far fronte alle connesse responsabilità per tutta la durata del suo mandato.

Torna a **Indice**

3 Trasferimento di dati verso paesi terzi e organismi internazionali



Premessa
Trasferimenti di dati verso paesi terzi e organismi internazionali

Il GDPR ha confermato l'approccio del legislatore europeo e nazionale rispetto ai trasferimenti di dati personali verso Paesi terzi. Mentre, infatti, vige la più assoluta libertà di circolazione dei dati personali all'interno dell'Ue e dello spazio economico europeo, posti sotto l'egida del GDPR, il trasferimento dei dati al di fuori dei confini dell'Ue è vietato a meno che il titolare possa far valere specifiche garanzie. Tuttavia, il GDPR fissa una gerarchia fra tali garanzie e introduce, al tempo stesso, nuovi strumenti per consentire ai titolari di procedere ai trasferimenti (come la certificazione o l'adesione a un codice di condotta). Più in generale, il GDPR ha reso maggiormente stringenti i requisiti che devono essere soddisfatti qualunque sia lo strumento di garanzia utilizzato per i trasferimenti di dati verso Paesi terzi, anche alla luce delle sentenze con cui la Corte di giustizia dell'Ue ha via via precisato i contorni della tutela che deve essere assicurata a ogni dato personale quando lascia il territorio di uno Stato membro dell'Ue.

L'adeguatezza del Paese terzo di destinazione è la prima delle garanzie in questione, alla quale il GDPR attribuisce chiaramente preminenza perché in questi casi la tutela è offerta dal sistema-Paese nel suo complesso, cioè dall'insieme dalla sua legislazione, delle prassi, dei meccanismi di ricorso giudiziario o amministrativo, tutti elementi che la Commissione europea prende in considerazione nel formulare la decisione di adeguatezza che le compete ai sensi del GDPR. Tuttavia, il sistema-Paese di destinazione dei dati deve garantire, a questo scopo, un livello di tutela "sostanzialmente equivalente" a quello dello Stato membro di provenienza. I Garanti hanno chiarito, attraverso le **raccomandazioni 1/2021**, quali siano gli standard da applicare ai fini della valutazione di adeguatezza che la Commissione può condurre rispetto ai trasferimenti di dati da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, ai sensi della direttiva 'polizia e giustizia' (2016/680); le raccomandazioni presentano un elenco di elementi da esaminare nel valutare l'adeguatezza del livello di protezione in tale ambito, tenendo conto della specificità e degli aspetti procedurali fissati nella direttiva nonché della giurisprudenza della CGUE in materia.

In tema di trasferimenti di dati all'estero e di strumenti di garanzia previsti al riguardo, la sentenza pronunciata dalla CGUE nel 2020 (causa C-311/18, cosiddetta 'Schrems II') ha prodotto conseguenze significative. Da un lato, la sentenza ha confermato la validità sostanziale delle clausole contrattuali tipo precedentemente adottate dalla Commissione europea, pur evidenziando la necessità per gli esportatori di dati di prevedere misure supplementari che integrino tali clausole in modo da assicurare l'effettività delle garanzie alla luce della legislazione e delle prassi nel paese terzo di destinazione; dall'altro, ha invalidato la decisione della Commissione relativa all'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy (*Privacy Shield*) proprio in considerazione della legislazione vigente negli USA. La sentenza ha spinto il Comitato a una prima reazione con la **Dichiarazione** del 17 luglio 2020 in cui veniva evidenziato il peso specifico considerevole della decisione della Corte e il suo spirito profondamente garantista, e quindi con una serie di **FAQ** pubblicate a breve giro, in cui si fornivano iniziali chiarimenti sulle conseguenze applicative della sentenza.

Uno dei primi effetti concreti della sentenza 'Schrems II' ha riguardato proprio un ripensamento da parte della Commissione europea delle garanzie offerte attraverso le clausole-tipo inserite in contratti stipulati fra esportatori di dati in Ue ed importatori (titolari o responsabili del trattamento) situati al di fuori dell'Ue. La Commissione ha infatti approvato un nuovo insieme di **clausole contrattuali tipo**, che tengono conto delle numerose osservazioni formulate dal Comitato europeo per la protezione dei dati, attraverso la **decisione di esecuzione 2021/914**. L'utilizzo delle nuove clausole (che ampliano e sostituiscono quelle precedentemente approvate dalla Commissione nel 2001 e nel 2010, in vigenza della direttiva 95/46, e fanno proprie le indicazioni fornite dalla Corte Ue), è obbligatorio per i contratti stipulati dopo il 27 settembre 2021.

Sempre alla luce della sentenza della Corte Ue nel caso C-311/18, è apparso assolutamente opportuno fornire indicazioni operative che aiutassero titolari e responsabili del trattamento nell'individuazione di possibili misure supplementari a integrazione delle garanzie contenute nello strumento di trasferimento volta per volta prescelto (BCR, clausole contrattuali tipo, altri strumenti), ove ciò risulti necessario alla luce della valutazione della legislazione del Paese terzo applicabile al trasferimento in questione. Pertanto, attraverso le **raccomandazioni 1/2020** sulle misure supplementari il Comitato ha voluto fornire specifiche indicazioni e un algoritmo di valutazione utili in questo senso a titolari e responsabili del trattamento in qualità di esportatori (siano essi enti privati o pubblici). Le raccomandazioni, partendo da un richiamo al principio dell'accountability, illustrano una sequenza di passi attraverso cui l'esportatore è accompagnato nell'individuazione degli strumenti più adeguati al trasferimento dei dati in un Paese terzo; in questo contesto, viene evidenziata l'importanza di esaminare, oltre alla legislazione, anche le pratiche relative agli accessi da parte delle autorità pubbliche dei Paesi terzi in cui si intende trasferire i dati al fine di valutare se tale legislazione e/o tali pratiche incidano in concreto sull'efficacia dello strumento di trasferimento prescelto. Le raccomandazioni indicano anche la possibilità che l'esportatore consideri l'esperienza dell'importatore in questo contesto, e ricordano la necessità di documentare la valutazione effettuata e lasciare la docu-

mentazione a disposizione delle autorità di protezione dei dati.

Si inseriscono in questo contesto anche le **raccomandazioni 2/2020 sulle garanzie essenziali europee relativamente alle misure di sorveglianza**, che in sostanza integrano le raccomandazioni 1/2020 sulle misure supplementari. L'obiettivo, in questo caso, è fornire agli esportatori di dati elementi utili a stabilire se il quadro giuridico nel Paese terzo in materia di accesso ai dati da parte delle autorità pubbliche (agenzie di intelligence o autorità di polizia/giudiziarie) per fini di sorveglianza configuri un'ingerenza giustificata nei diritti alla vita privata e alla protezione dei dati personali, e non sia quindi in contrasto con gli impegni assunti dall'esportatore e dall'importatore attraverso lo strumento utilizzato per il trasferimento (BCR, clausole contrattuali, codici di condotta, certificazioni, accordi internazionali o amministrativi). Le raccomandazioni evidenziano, in particolare, che la valutazione delle garanzie essenziali europee deve essere effettuata in modo olistico, trattandosi di garanzie strettamente interconnesse.

La sentenza 'Schrems II' ha inciso anche sui trasferimenti di dati posti in essere da soggetti pubblici, sia quando questi si avvalgono di responsabili (o sub-responsabili) del trattamento stabiliti in Paesi terzi, sia quando i dati sono trasferiti direttamente a soggetti pubblici nel Paese terzo. Con riferimento a tale ultima tipologia di trasferimenti, il Comitato ha quindi elaborato apposite **linee guida (2/2020) per il trasferimento di dati a soggetti pubblici nei Paesi terzi o ad organizzazioni internazionali**, che recano indicazioni in ordine alle garanzie adeguate che dovranno essere contenute sia negli accordi internazionali vincolanti per gli Stati (per i quali non c'è bisogno di autorizzazione da parte dell'autorità di protezione dei dati) sia negli accordi amministrativi tra autorità pubbliche o organismi pubblici che dovranno essere autorizzati dalle autorità di protezione dei dati dopo aver ottenuto il parere del Comitato ex art. 64, par. 2, del GDPR. Tra gli elementi essenziali che devono figurare negli accordi, le raccomandazioni indicano, in particolare, definizioni in linea con quelle contenute nel RGPD, disposizioni in materia di trasparenza per gli interessati, l'espressa previsione dei principi di protezione dei dati e dei diritti degli interessati (compreso il diritto ad una tutela effettiva), disposizioni restrittive in materia di trasferimenti ulteriori e misure di sicurezza. Le linee guida chiariscono che ciascun accordo verrà valutato caso per caso e ciò consentirà anche di individuare, ove necessario, garanzie specifiche per assicurare la tutela effettiva agli interessati. Alla luce della sentenza Schrems II, si richiama l'attenzione sulla necessità per le autorità pubbliche europee di effettuare, prima di concludere definitivamente gli accordi in questione, una valutazione del livello di protezione nel Paese dell'importatore, compresa una verifica circa la possibilità che le garanzie concordate siano rispettate in concreto.

Da segnalare, infine, **le linee guida 4/2021 sui codici di condotta come strumenti per il trasferimento dei dati all'estero**, che permettono di chiarire sia l'ambito applicativo sia i contenuti di questo nuovo strumento. Le linee guida chiariscono in proposito che ai codici da utilizzare come strumento per il trasferimento dei dati possono aderire i titolari o i responsabili del trattamento, non soggetti al RGPD, situati in paesi terzi (importatori). I codici possono essere uti-

lizzati inoltre, senza alcuna necessità di adesione, dai titolari/responsabili del trattamento soggetti al RGPD (vale a dire gli esportatori) per adempiere agli obblighi posti dal Capo V del RGPD in caso di trasferimenti verso tale importatore. Quanto agli elementi che devono figurare nei codici di condotta in questione, le linee guida menzionano i diritti per gli interessati, principi di protezione dei dati analoghi a quelli contenuti nel RGPD, misure di accountability da porre in essere, ecc. e ricordano gli impegni vincolanti e azionabili che l'importatore, mediante contratto o altro strumento vincolante, deve assumere per assicurare l'applicazione delle garanzie contenute nel codice di condotta cui aderisce.

Linee guida 2/2020 sull'articolo 46, paragrafo 2, lettera a), e paragrafo 3, lettera b), del regolamento 2016/679 per i trasferimenti di dati personali tra autorità ed organismi pubblici del SEE e di paesi non appartenenti al SEE

Versione 2.0

Adottate il 15 dicembre 2020

Cronologia delle versioni

Versione 2.0	15 dicembre 2020	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	18 febbraio 2020	Adozione delle linee guida per la consultazione pubblica

Indice

1 Informazioni generali
- 1.1 Finalità
- 1.2 Regole generali applicabili ai trasferimenti internazionali
- 1.3 Definizione di autorità o organismo pubblico

2 Raccomandazioni generali per le garanzie adeguate ai sensi dell'articolo 46, paragrafo 2, lettera a), e paragrafo 3, lettera b), del GDPR
- 2.1 Finalità e ambito di applicazione
- 2.2 Definizioni
- 2.3 Principi di protezione dei dati
  - 2.3.1 Principio di limitazione delle finalità
  - 2.3.2 Accuratezza dei dati e principi di minimizzazione
  - 2.3.3 Principio di limitazione della conservazione
  - 2.3.4 Sicurezza e riservatezza dei dati
- 2.4 Diritti degli interessati
  - 2.4.1 Diritto alla trasparenza
  - 2.4.2 Diritti di accesso, rettifica, cancellazione, limitazione di trattamento e opposizione
  - 2.4.3 Processo decisionale automatizzato relativo alle persone fisiche
  - 2.4.4 Diritto di ricorso
  - 2.4.5 Limitazioni ai diritti degli interessati
- 2.5 Limitazioni ai trasferimenti successivi e alla condivisione dei dati (compresa la divulgazione e l'accesso del governo)
- 2.6 Dati sensibili
- 2.7 Meccanismi di ricorso
- 2.8 Meccanismi di controllo
- 2.9 Clausola di risoluzione

3 Informazioni specifiche sull'articolo 46 del GDPR
- 3.1 Informazioni specifiche sugli strumenti giuridicamente vincolanti e aventi efficacia esecutiva - Articolo 46, paragrafo 2, lettera a), del GDPR
- 3.2 Informazioni specifiche sugli accordi amministrativi - [Articolo 46, paragrafo 3, lettera b), del GDPR]

4 Questioni procedurali

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati),

visto l'accordo sullo Spazio economico europeo (SEE), in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

visti gli articoli 12 e 22 del proprio regolamento interno,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

1. INFORMAZIONI GENERALI

1.1 FINALITÀ

1. Il presente documento mira a fornire una guida sull'applicazione dell'articolo 46, paragrafo 2, lettera a), e paragrafo 3, lettera b), del regolamento generale sulla protezione dei dati ("GDPR") per i trasferimenti di dati personali da autorità o organismi pubblici del SEE (di seguito "organismi pubblici") ad organismi pubblici di paesi terzi od organizzazioni internazionali, nella misura in cui ad essi non si applichi un accertamento di adeguatezza adottato dalla Commissione europea[2]. Gli organismi pubblici possono scegliere di avvalersi dei meccanismi che il GDPR ritiene più adeguati alla loro situazione, ma sono anche liberi di fare affidamento su altri strumenti pertinenti che prevedano adeguate garanzie ai sensi dell'articolo 46 del GDPR.
2. Le linee guida intendono fornire un'indicazione delle aspettative del Comitato europeo per la protezione dei dati ("EDPB") sulle garanzie che devono essere attuate da uno strumento giuridicamente vincolante e avente efficacia esecutiva tra organismi pubblici, ai sensi dell'articolo 46, paragrafo 2, lettera a), del GDPR o, previa autorizzazione dell'autorità di controllo competente, da disposizioni da inserire in accordi amministrativi tra organismi pubblici ai sensi dell'articolo 46, paragrafo 3, lettera b), del GDPR[3]. L'EDPB raccomanda vivamente alle parti di utilizzare le linee guida come riferimento già in fase iniziale, quando si prevede di concludere o modificare tali strumenti o accordi[4].
3. Le linee guida devono essere lette congiuntamente ad altri documenti precedenti dell'EDPB (compresi i documenti approvati dal suo predecessore, il gruppo di lavoro "Articolo 29"[5]) sulle questioni centrali dell'ambito di applicazione territoriale e dei trasferimenti di dati personali verso paesi terzi[6]. Le linee guida saranno sottoposte a riesame e, se necessario, aggiornate, sulla base dell'esperienza pratica maturata dall'applicazione del GDPR.
4. Le presenti linee guida riguardano i trasferimenti internazionali di dati tra organismi pubblici effettuati per vari scopi di cooperazione amministrativa che rientrano nell'ambito di applicazione del GDPR. Di conseguenza e in conformità con l'articolo 2, paragrafo 2, del GDPR, non riguardano i trasferimenti nel settore della sicurezza pubblica, della difesa o della sicurezza dello Stato. Inoltre non si occupano del trattamento e dei trasferimenti dei dati da parte delle autorità competenti a fini giudiziari e di polizia, essendo tale settore disciplinato da uno strumento specifico e distinto, la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie[7]. Infine le linee guida si concentrano solo sui trasferimenti tra organismi pubblici e non riguardano i trasferimenti di dati personali fra un organismo pubblico e un soggetto privato o fra un soggetto privato e un organismo pubblico.

1.2 REGOLE GENERALI APPLICABILI AI TRASFERIMENTI INTERNAZIONALI

5. Ai sensi dell'articolo 44 del GDPR, l'esportatore di dati che trasferisce dati personali verso paesi terzi o organizzazioni internazionali, oltre a rispettare il capo V del GDPR, deve anche soddisfare le condizioni delle altre disposizioni del GDPR. In particolare, ogni attività di trattamento deve essere conforme ai principi di protezione dei dati di cui all'articolo 5 del GDPR, essere lecita ai sensi dell'articolo 6 del GDPR e rispettare l'articolo 9 del GDPR in caso di categorie particolari di dati. Pertanto occorre seguire un approccio in due fasi: in primo luogo, deve essere applicata una base giuridica al trattamento dei dati in quanto tale, insieme a tutte le disposizioni pertinenti del GDPR; nella seconda fase, devono essere rispettate le disposizioni del capo V del GDPR.
6. L'articolo 46 del GDPR specifica che "*[i]n mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi*". Tali garanzie adeguate possono essere previste da uno strumento giuridicamente vincolante e avente efficacia esecutiva tra organismi pubblici [articolo 46, paragrafo 2, lettera a), del GDPR] o, previa autorizzazione dell'autorità di controllo competente, da disposizioni da inserire in accordi amministrativi tra organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati [articolo 46, paragrafo 3, lettera b), del GDPR]. Come chiarito dalla Corte di giustizia dell'Unione europea, tali garanzie adeguate devono essere idonee a garantire che le persone i cui dati personali sono trasferiti godano di un livello di protezione sostanzialmente equivalente a quello garantito all'interno del SEE[8].
7. Oltre a questa soluzione e in sua assenza, l'articolo 49 del GDPR prevede anche un numero limitato di situazioni specifiche in cui possono aver luogo trasferimenti internazionali di dati pur non essendovi alcun accertamento di adeguatezza da parte della Commissione europea[9]. In particolare, una deroga riguarda i trasferimenti necessari per importanti motivi di interesse pubblico riconosciuti dal diritto dell'Unione o dal diritto dello Stato membro a cui è soggetto il titolare del trattamento, anche nello spirito di reciprocità della cooperazione internazionale[10]. Tuttavia, come spiegato in precedenti linee guida emesse dall'EDPB, le deroghe previste dall'articolo 49 del GDPR devono essere interpretate in modo restrittivo e riguardano principalmente le attività di trattamento che sono occasionali e non ripetitive[11].

1.3 DEFINIZIONE DI AUTORITÀ O ORGANISMO PUBBLICO

8. Il GDPR non contiene la definizione di "autorità o organismo pubblico". L'EDPB ritiene che questa nozione sia sufficientemente ampia da coprire sia gli organismi pubblici nei paesi terzi, sia le organizzazioni internazionali[12]. Per quanto riguarda gli organismi pubblici nei paesi terzi, la nozione deve essere determinata in base al diritto interno. Di conseguenza, gli organismi

pubblici includono autorità governative a diversi livelli (ad es. autorità nazionali, regionali e locali), tuttavia possono anche includere altri organismi di diritto pubblico (ad es. agenzie esecutive, università, ospedali, ecc.)[13]. Ai sensi dell'articolo 4, punto 26, del GDPR, per "organizzazione internazionale" s'intende un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due Stati.

9. L'EDPB ricorda che l'applicazione del GDPR lascia impregiudicate le disposizioni di diritto internazionale, come quelle che regolano i privilegi e le immunità delle organizzazioni internazionali. Allo stesso tempo, è importante ricordare che qualsiasi organismo pubblico del SEE che trasferisce dati verso organizzazioni internazionali deve rispettare le regole del GDPR per i trasferimenti verso paesi terzi o organizzazioni internazionali.[14]

2. RACCOMANDAZIONI GENERALI PER LE GARANZIE ADEGUATE AI SENSI DELL'ARTICOLO 46, PARAGRAFO 2, LETTERA A), E PARAGRAFO 3, LETTERA B), DEL GDPR

10. A differenza dell'articolo 26, paragrafo 2, della direttiva 95/46/CE, l'articolo 46 del GDPR prevede ulteriori garanzie adeguate come strumenti per i trasferimenti tra organismi pubblici:

    (i) uno strumento giuridicamente vincolante e avente efficacia esecutiva, articolo 46, paragrafo 2, lettera a), del GDPR, o

    (ii) disposizioni da inserire in accordi amministrativi tra organismi pubblici, articolo 46, paragrafo 3, lettera b), del GDPR.

    Detti strumenti e accordi possono avere natura bilaterale o multilaterale.

11. La sezione seguente fornisce alcune raccomandazioni generali per contribuire a garantire che gli strumenti giuridicamente vincolanti o gli accordi amministrativi (di seguito "accordi internazionali") tra organismi pubblici siano conformi al GDPR.

12. Sebbene l'articolo 46 e il considerando 108 del GDPR non forniscano indicazioni specifiche sulle garanzie da includere in tali accordi internazionali, tenendo conto dell'articolo 44 del GDPR[15] e della recente giurisprudenza della Corte di giustizia dell'Unione europea[16], l'EDPB ha elaborato un elenco delle garanzie minime da includere negli accordi internazionali tra organismi pubblici conformemente all'articolo 46, paragrafo 2, lettera a), o all'articolo 46, paragrafo 3, lettera b), del GDPR. Le suddette garanzie mirano ad assicurare che il livello di protezione delle persone fisiche ai sensi del GDPR non sia compromesso se i loro dati personali vengono trasferiti al di fuori del SEE e che gli interessati godano di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE dal GDPR[17].

13. In conformità con la recente giurisprudenza della Corte di giustizia dell'Unione europea[18], è responsabilità dell'organismo pubblico trasferente in uno Stato membro, se necessario con l'aiuto dell'organismo pubblico destinata-

rio, valutare se il livello di protezione richiesto dal diritto dell'UE sia rispettato nel paese terzo, al fine di determinare se l'elenco delle garanzie incluso nell'accordo internazionale possa essere rispettato nella pratica, tenendo conto delle possibili interferenze nel rispetto di tali garanzie derivanti dalla legislazione del paese terzo.

14. A tale riguardo, va anche notato che, per assicurare le garanzie elencate nelle presenti linee guida, gli accordi internazionali possono basarsi su elementi già esistenti nel diritto nazionale di un paese terzo o sulle norme interne/sul quadro normativo di un'organizzazione internazionale.

2.1 FINALITÀ E AMBITO DI APPLICAZIONE

15. Gli accordi internazionali dovrebbero definire il rispettivo ambito di applicazione, e le loro finalità dovrebbero essere determinate in modo esplicito e specifico. Inoltre dovrebbero indicare chiaramente le categorie di dati personali interessate e la tipologia dei trattamenti riferiti ai dati personali trasferiti e trattati ai sensi dell'accordo.

2.2 DEFINIZIONI

16. Gli accordi internazionali dovrebbero contenere le definizioni dei concetti e dei diritti basilari relativi ai dati personali, in linea con il GDPR e in quanto rilevanti per lo specifico accordo. A titolo di esempio, tali accordi, ove vi facciano riferimento, dovrebbero includere le seguenti importanti definizioni: "dati personali", "trattamento dei dati personali", "titolare del trattamento", "responsabile del trattamento", "destinatario" e "dati sensibili".

2.3 PRINCIPI DI PROTEZIONE DEI DATI

17. Gli accordi internazionali devono contenere una formulazione specifica che imponga alle parti il rispetto dei principi fondamentali della protezione dei dati.

2.3.1 PRINCIPIO DI LIMITAZIONE DELLE FINALITÀ

18. Gli accordi internazionali devono specificare le finalità per le quali i dati personali devono essere trasferiti e trattati, comprese le finalità compatibili per trattamenti ulteriori, nonché garantire che i dati non saranno ulteriormente trattati per finalità incompatibili. Le finalità compatibili possono includere la conservazione a fini di archiviazione nel pubblico interesse, nonché il trattamento a fini di ricerca scientifica o storica o a fini statistici. Si raccomanda, per maggiore chiarezza, di elencare le specifiche finalità del trattamento e del trasferimento dei dati nell'accordo internazionale stesso.

19. Per evitare qualsiasi rischio di "function creep" (estensione indebita delle funzionalità), tali accordi dovrebbero inoltre specificare che i dati trasferiti non possono essere utilizzati per finalità diverse da quelle espressamente menzionate nell'accordo, ad eccezione di quanto stabilito qui di seguito.
20. Se entrambe le parti dell'accordo internazionale desiderano consentire all'organismo pubblico destinatario un altro uso compatibile dei dati personali trasmessi, l'ulteriore utilizzo da parte dell'organismo pubblico destinatario è consentito solo se compatibile con quello originale e se precedentemente notificato all'organismo pubblico trasferente, che può opporvisi per motivi specifici.

2.3.2 ACCURATEZZA DEI DATI E PRINCIPI DI MINIMIZZAZIONE

21. L'accordo internazionale deve specificare che i dati trasferiti e successivamente trattati devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali vengono trasmessi e successivamente trattati.
22. In pratica, questo principio di minimizzazione dei dati è importante per evitare il trasferimento di dati personali inadeguati o eccessivi.
23. Inoltre i dati dovrebbero essere esatti e aggiornati, tenendo conto delle finalità per le quali vengono trattati. Un accordo internazionale deve quindi prevedere che la parte trasferente garantisca che i dati personali trasferiti in base all'accordo siano esatti e, ove applicabile, aggiornati. Inoltre l'accordo dovrebbe prevedere che, se una delle parti viene a conoscenza del fatto che sono stati trasmessi o sono trattati dati inesatti o non aggiornati, detta parte deve informare senza indugio l'altra parte. Infine, l'accordo dovrebbe garantire che, qualora sia confermato che i dati trasmessi o trattati sono inesatti, ciascuna parte che tratta i dati adotti ogni ragionevole misura per rettificare o cancellare le informazioni.

2.3.3 PRINCIPIO DI LIMITAZIONE DELLA CONSERVAZIONE

24. Le parti devono garantire che l'accordo internazionale contenga una clausola sulla conservazione dei dati. Tale clausola dovrebbe specificare in particolare che i dati personali non devono essere conservati a tempo indeterminato, ma in una forma che consenta l'identificazione degli interessati solo per il tempo necessario alle finalità per le quali sono stati trasferiti e successivamente trattati. Ciò può includere la conservazione a fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici, a condizione che siano messe in atto misure tecniche e organizzative appropriate per salvaguardare i diritti e le libertà degli interessati, come misure tecniche aggiuntive (ad esempio misure di sicurezza, pseudonimizzazione) e limitazioni all'accesso. Quando il periodo massimo di conservazione non è già fissato dalla legislazione nazionale o dalle norme interne/dal quadro nor-

mativo di un'organizzazione internazionale, esso dovrebbe essere indicato nel testo dell'accordo.

2.3.4 SICUREZZA E RISERVATEZZA DEI DATI

25. Le parti dovrebbero impegnarsi a garantire la sicurezza e la riservatezza del trattamento dei dati personali e dei trasferimenti che effettuano.

    In particolare, le parti dovrebbero impegnarsi a mettere in atto misure tecniche e organizzative adeguate per proteggere i dati personali da accessi accidentali o illeciti, distruzione, perdita, alterazione o divulgazione non autorizzata. Tali misure possono includere, ad esempio, la cifratura anche in transito, la pseudonimizzazione, la marcatura delle informazioni come dati personali trasferiti dal SEE, la limitazione del numero di persone che hanno accesso ai dati personali, un'archiviazione sicura dei dati personali o l'attuazione di politiche progettate per garantire la conservazione dei dati personali in modo sicuro e riservato.

    Il livello di sicurezza dovrebbe tenere in considerazione i rischi, lo stato dell'arte e i relativi costi.

26. L'accordo internazionale può inoltre specificare che, se una delle parti viene a conoscenza di una violazione dei dati personali, informerà l'altra o le altre parti il prima possibile e utilizzerà mezzi ragionevoli e appropriati per porre rimedio alla violazione dei dati personali e ridurre al minimo i potenziali effetti negativi, anche comunicando all'interessato la violazione dei dati personali, senza indebito ritardo, laddove tale violazione dei dati personali possa comportare un rischio elevato per i diritti e le libertà della persona fisica.

    Si raccomanda che la tempistica della notifica in caso di violazione dei dati personali e le procedure per la comunicazione all'interessato siano definite nell'accordo internazionale.

2.4 DIRITTI DEGLI INTERESSATI

27. L'accordo internazionale deve garantire diritti effettivi e azionabili per gli interessati come specificato nell'articolo 46, paragrafo 1, e nel considerando 108 del GDPR.

28. I diritti di cui godono gli interessati, compresi gli impegni specifici assunti dalle parti per garantire tali diritti, dovrebbero essere elencati nell'accordo. Per essere efficace, l'accordo internazionale deve prevedere meccanismi che garantiscano la loro applicazione nella pratica. Inoltre qualsiasi violazione dei diritti dell'interessato deve comportare un rimedio appropriato.

2.4.1 DIRITTO ALLA TRASPARENZA

29. Le parti devono garantire che l'accordo internazionale contenga una formu-

lazione chiara che descriva gli obblighi di trasparenza delle parti.

30. Tali obblighi dovrebbero includere, da un lato, una informativa generale contenente almeno informazioni su come e perché gli organismi pubblici possono trattare e trasferire dati personali, lo strumento pertinente utilizzato per il trasferimento, i soggetti a cui tali dati possono essere trasferiti, i diritti di cui godono gli interessati e le limitazioni applicabili, i meccanismi di ricorso disponibili e le informazioni necessarie per presentare una denuncia o un reclamo.

31. Tuttavia è importante ricordare che, per l'organismo pubblico trasferente, non sarà sufficiente pubblicare un'informativa generale sul proprio sito web. Gli interessati dovranno essere informati in via individuale dall'organismo pubblico trasferente in conformità degli obblighi di informazione di cui agli articoli 13 e 14 del GDPR[19].

    L'accordo internazionale può anche prevedere alcune eccezioni a tali informative individuali. Dette eccezioni sono limitate e dovrebbero essere in linea con quelle previste dall'articolo 14, paragrafo 5, del GDPR, ad esempio laddove l'interessato disponga già delle informazioni o la fornitura di tali informazioni risulti impossibile o implichi uno sforzo sproporzionato.

32. Le parti devono impegnarsi a mettere l'accordo internazionale a disposizione degli interessati, su richiesta, e a mettere a disposizione del pubblico sul rispettivo sito web l'accordo internazionale o le disposizioni pertinenti che prevedono adeguate garanzie. Nella misura necessaria per proteggere informazioni sensibili o altre informazioni riservate, il testo pertinente dell'accordo internazionale può essere omesso prima di condividere una copia o di renderlo disponibile al pubblico. Ove necessario per consentire all'interessato di comprendere il contenuto dell'accordo internazionale, le parti devono fornire una sintesi comprensibile dello stesso.

2.4.2 DIRITTI DI ACCESSO, RETTIFICA, CANCELLAZIONE, LIMITAZIONE DI TRATTAMENTO E OPPOSIZIONE

33. L'accordo internazionale dovrebbe salvaguardare il diritto dell'interessato di ottenere informazioni e l'accesso a tutti i dati personali trattati che lo riguardano, il diritto di rettifica, cancellazione e limitazione del trattamento e, se del caso, il diritto di opporsi al trattamento dei dati per motivi relativi alla sua situazione particolare.

34. Per quanto riguarda il diritto di accesso, l'accordo internazionale dovrebbe specificare che le persone hanno il diritto nei confronti dell'organismo pubblico destinatario di ottenere conferma che i propri dati personali siano o meno trattati e, se del caso, di accedere a tali dati, nonché a specifiche informazioni riguardanti il trattamento, ivi comprese le finalità del trattamento, le categorie di dati personali interessate, i destinatari a cui i dati personali vengono comunicati, il periodo di conservazione previsto e le possibilità di ricorso.

35. L'accordo dovrebbe inoltre specificare quando questi diritti possono essere invocati e includere le modalità di esercizio di tali diritti da parte degli interessati nei confronti di entrambe le parti, nonché le modalità di risposta delle parti a tali richieste. Ad esempio, per quanto riguarda la cancellazione, l'accordo internazionale potrebbe stabilire che i dati debbano essere cancellati se le informazioni sono state trattate illecitamente o non sono più necessarie ai fini del trattamento. Inoltre l'accordo internazionale dovrebbe stabilire che le parti risponderanno in modo ragionevole e tempestivo alle richieste degli interessati. L'accordo internazionale potrebbe anche stabilire che le parti possono adottare misure appropriate, come l'addebito di contributi spese ragionevoli per coprire i costi amministrativi qualora le richieste di un interessato siano manifestamente infondate o eccessive, in particolare a causa del loro carattere ripetitivo.

36. L'accordo internazionale dovrebbe altresì imporre all'organismo pubblico trasferente l'obbligo di fornire all'interessato, una volta che i suoi dati personali siano stati trasferiti, le informazioni relative all'azione intrapresa riguardo a una sua richiesta in virtù dei diritti previsti dall'accordo internazionale, senza indebito ritardo, fissando un termine appropriato (ad esempio un mese). Infine, se le parti non ottemperano alla richiesta dell'interessato, quest'ultimo dovrebbe essere informato senza indebito ritardo, entro un termine appropriato (ad esempio entro un mese dal ricevimento della richiesta), dei motivi dell'inottemperanza e della possibilità di proporre reclamo e di proporre ricorso giurisdizionale.

37. L'accordo internazionale può anche prevedere eccezioni a tali diritti. Ad esempio, potrebbero essere previste eccezioni al diritto di accesso e di cancellazione, come quelle previste dall'articolo 15, paragrafo 4, e dall'articolo 17, paragrafo 3, del GDPR. Analogamente, potrebbero essere previste eccezioni ai diritti delle persone se i dati personali sono trattati a fini di ricerca scientifica o storica, a fini statistici o di archiviazione, nella misura in cui tali diritti potrebbero rendere impossibile o pregiudicare gravemente il conseguimento di tali finalità, e a condizione che siano messe in atto adeguate garanzie (ad esempio misure tecniche e organizzative, compresa la pseudonimizzazione). Infine l'accordo può prevedere che le parti possano rifiutarsi di dare seguito a una richiesta manifestamente infondata o eccessiva.

2.4.3 PROCESSO DECISIONALE AUTOMATIZZATO RELATIVO ALLE PERSONE FISICHE

38. Se pertinente nel caso specifico, gli accordi internazionali dovrebbero contenere, in generale, una clausola in cui si afferma che l'organismo pubblico destinatario non prenderà una decisione basata unicamente su di un processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione, che produca effetti giuridici riguardanti l'interessato in questione o che incida in modo analogo sulla sua persona. Laddove le finalità del trasferimento includano la possibilità per l'organismo pubblico destinatario di prendere decisioni unicamente sulla base di un processo decisionale automatizzato ai sensi dell'articolo 22 del GDPR, ciò dovrebbe avvenire solo a de-

terminate condizioni stabilite nell'accordo internazionale, come la necessità di ottenere il consenso esplicito dell'interessato. Se la decisione non è conforme a tali condizioni, l'interessato dovrebbe avere il diritto di non esservi sottoposto. Laddove l'accordo internazionale consenta un processo decisionale automatizzato relativo alle persone fisiche, esso dovrebbe, in ogni caso, prevedere le garanzie necessarie, compreso il diritto di essere informati sui motivi specifici alla base della decisione e sulla logica utilizzata, di rettificare informazioni inesatte o incomplete e di contestare la decisione e ottenere l'intervento umano.

2.4.4 DIRITTO DI RICORSO

39. I diritti tutelati dell'interessato devono essere effettivi e azionabili. Pertanto l'interessato deve avere accesso a mezzi di ricorso. Diversi esempi di modalità per offrire meccanismi di ricorso sono indicati di seguito nelle sezioni 2.7 e 3.

2.4.5 LIMITAZIONI AI DIRITTI DEGLI INTERESSATI

40. L'accordo internazionale può anche prevedere limitazioni ai diritti degli interessati. Tali limitazioni dovrebbero essere in linea con quelle previste dall'articolo 23 del GDPR. Le limitazioni devono essere una misura necessaria e proporzionata in una società democratica per salvaguardare obiettivi importanti di interesse pubblico, in linea con quelli elencati nell'articolo 23, paragrafo 1, del GDPR, tra cui i diritti e la libertà altrui, la sicurezza nazionale, la difesa o la prevenzione, l'indagine, l'accertamento o il perseguimento di reati. Tali limitazioni devono essere previste dalla legge o, nel caso di organizzazioni internazionali, dalle norme interne applicabili/dal quadro normativo applicabile e vigono finché persiste il motivo per cui sono state stabilite.

2.5 LIMITAZIONI AI TRASFERIMENTI SUCCESSIVI E ALLA CONDIVISIONE DEI DATI (COMPRESA LA COMUNICAZIONE E L'ACCESSO DA PARTE DI ORGANISMI GOVERNATIVI)

41. I trasferimenti successivi da parte dell'organismo pubblico destinatario o dell'organizzazione internazionale destinataria verso destinatari non vincolati dall'accordo dovrebbero, di regola, essere specificamente esclusi dall'accordo internazionale. A seconda dell'oggetto e delle circostanze particolari, le parti potrebbero ritenere necessario consentire trasferimenti successivi. In questo caso, a condizione che sia rispettato il principio di limitazione delle finalità[20], l'accordo internazionale dovrebbe prevedere che tali trasferimenti successivi possano aver luogo solo se l'organismo pubblico trasferente ha dato la sua previa ed espressa autorizzazione e le terze parti destinatarie si impegnano a rispettare gli stessi principi e garanzie di protezione dei dati inclusi nell'accordo internazionale. Ciò dovrebbe includere l'impegno a fornire agli interessati gli stessi diritti e garanzie di protezione dei dati previsti

dall'accordo internazionale al fine di garantire che il livello di protezione non si riduca a seguito del trasferimento successivo dei dati.

42. Di norma, le stesse garanzie previste per i trasferimenti successivi dovrebbero applicarsi alla condivisione dei dati personali all'interno del paese destinatario, vale a dire che l'accordo internazionale deve escludere tale condivisione successiva e che eventuali deroghe dovrebbero in generale essere consentite solo se l'organismo pubblico trasferente ha dato la sua previa ed espressa autorizzazione e le terze parti destinatarie si impegnano a rispettare gli stessi principi e le stesse garanzie di protezione dei dati inclusi nell'accordo internazionale.

43. Si raccomanda che, prima di richiedere l'espressa autorizzazione dell'organismo pubblico trasferente, l'organismo pubblico destinatario o l'organizzazione internazionale destinataria fornisca informazioni sufficienti sulla tipologia dei dati personali che intende trasferire/condividere, i motivi e le finalità per i quali ritiene sia necessario trasferire/condividere i dati personali nonché, in caso di trasferimenti successivi, i paesi o le organizzazioni internazionali a cui intende trasferire successivamente i dati personali, in modo da poter valutare la legislazione del paese terzo o, nel caso di organizzazioni internazionali, le norme interne applicabili/il quadro normativo applicabile.

44. Nei casi in cui sia necessario consentire la condivisione di dati personali con una terza parte nello stesso paese dell'organismo pubblico destinatario o altra organizzazione internazionale, la condivisione potrebbe essere consentita in circostanze specifiche con la previa ed espressa autorizzazione dell'organismo pubblico trasferente oppure in presenza di un impegno vincolante da parte del terzo destinatario a rispettare i principi e le garanzie inclusi nell'accordo internazionale.

45. Inoltre l'accordo internazionale potrebbe specificare le circostanze eccezionali in cui la condivisione successiva potrebbe avvenire senza previa autorizzazione o senza gli impegni sopra menzionati, in linea con le deroghe elencate nell'articolo 49 del GDPR, ad esempio qualora la condivisione in questione sia necessaria per proteggere interessi vitali dell'interessato o di altre persone o per accertare, esercitare o difendere un diritto in sede giudiziaria. Tali circostanze eccezionali potrebbero anche verificarsi se la condivisione successiva è richiesta dalla legge della parte destinataria per indagini/procedimenti giudiziari direttamente correlati.

46. Nei casi summenzionati l'accordo internazionale dovrebbe indicare chiaramente le circostanze specifiche ed eccezionali in cui è consentita tale condivisione dei dati. L'organismo pubblico destinatario o l'organizzazione internazionale destinataria dovrebbero inoltre essere obbligati a inviare una notifica all'organismo pubblico trasferente, prima della condivisione, contenente informazioni sui dati condivisi, sulla terza parte destinataria e sulla base giuridica della condivisione. A sua volta, l'organismo pubblico trasferente dovrebbe tenere un registro di tali notifiche dell'organismo pubblico destinatario o dell'organizzazione internazionale destinataria e fornire su richiesta queste informazioni alla sua autorità di controllo. Qualora fornire

tale notifica prima della condivisione pregiudichi gli obblighi di riservatezza previsti dalla legge, ad esempio per tutelare la riservatezza di un'indagine, le informazioni specifiche dovrebbero essere fornite il prima possibile dopo la condivisione. In tal caso, dovrebbero essere fornite periodicamente, all'organismo trasferente, informazioni generali sulla tipologia delle richieste ricevute in un determinato periodo, comprese le informazioni sulle categorie di dati richiesti, sull'organismo richiedente e sulla base giuridica per la comunicazione.

47. In tutti gli scenari di cui sopra, l'accordo internazionale dovrebbe consentire solo la comunicazione ad altre autorità pubbliche, nel paese terzo dell'organismo pubblico destinatario, di dati personali che non eccedano quanto necessario e proporzionato in una società democratica per salvaguardare obiettivi importanti di interesse pubblico, in linea con quelli elencati nell'articolo 23, paragrafo 1, del GDPR e in conformità della giurisprudenza della Corte di giustizia dell'Unione europea. Al fine di valutare un possibile accesso da parte delle autorità pubbliche di paesi terzi a fini di sorveglianza, l'autorità pubblica trasferente dovrebbe tenere conto degli elementi richiamati nelle quattro garanzie essenziali europee[21]. Queste ultime includono la disponibilità di un ricorso efficace per gli interessati nel paese terzo dell'organismo pubblico destinatario se le autorità pubbliche accedono ai loro dati personali[22]. In caso di trasferimenti a organizzazioni internazionali, qualsiasi accesso di questo tipo deve essere conforme al diritto internazionale e non deve pregiudicare in particolare i privilegi e le immunità dell'organizzazione internazionale.

48. A seconda del caso specifico, può essere utile prevedere che l'accordo internazionale comprenda un allegato in cui siano specificate le leggi che disciplinano la condivisione successiva con altri organismi pubblici, anche a fini di sorveglianza, nel paese di destinazione. Eventuali modifiche di tale allegato dovrebbero essere notificate alla parte trasferente entro un periodo predefinito.

2.6 DATI SENSIBILI

49. Se un accordo internazionale prevede il trasferimento di dati personali sensibili ai sensi dell'articolo 9, paragrafo 1, del GDPR, dovrebbero essere incluse ulteriori garanzie per gestire i rischi specifici, e tali garanzie dovranno essere attuate dall'organismo pubblico destinatario o dall'organizzazione internazionale destinataria. Le garanzie in questione potrebbero prevedere, ad esempio, limitazioni all'accesso, alle finalità per le quali le informazioni possono essere trattate, ai trasferimenti successivi, ecc., oppure garanzie specifiche, ad esempio misure di sicurezza aggiuntive, che richiedono una formazione specializzata per il personale autorizzato ad accedere alle informazioni.

2.7 MECCANISMI DI RICORSO

50. Al fine di garantire i diritti azionabili ed effettivi degli interessati, l'accordo

internazionale deve prevedere un sistema che consenta agli interessati di continuare a beneficiare di meccanismi di ricorso dopo che i loro dati sono stati trasferiti a un paese non SEE o a un'organizzazione internazionale. Tali meccanismi devono prevedere la possibilità di ricorso per le persone che sono interessate dal mancato rispetto delle disposizioni dello strumento scelto e quindi la possibilità per gli interessati, i cui dati personali sono stati trasferiti dal SEE, di presentare reclami in merito a tale inosservanza e di ottenerne la risoluzione. In particolare, all'interessato deve essere garantito un percorso efficace per presentare reclamo agli organismi pubblici parti dell'accordo internazionale e (direttamente o dopo essersi rivolto alla parte interessata) a un meccanismo di controllo indipendente. Inoltre dovrebbe essere disponibile, in linea di principio, un ricorso giurisdizionale.

51. In primo luogo, l'organismo pubblico destinatario dovrebbe impegnarsi a mettere in atto un meccanismo per gestire e risolvere in modo efficace e tempestivo i reclami degli interessati in merito al rispetto delle garanzie concordate per la protezione dei dati. Inoltre gli interessati dovrebbero avere la possibilità di ottenere un ricorso amministrativo efficace dinanzi a un organismo di controllo indipendente, inclusa, se esistente, un'autorità indipendente per la protezione dei dati[23].

52. In secondo luogo, l'accordo dovrebbe consentire un ricorso giurisdizionale che preveda il risarcimento dei danni, sia materiali che immateriali, a seguito del trattamento illecito dei dati personali. Se non è possibile garantire un ricorso giurisdizionale effettivo, ad esempio a causa di limitazioni del diritto interno o dello status specifico dell'organismo pubblico destinatario, ad esempio organizzazioni internazionali, l'accordo internazionale deve prevedere garanzie alternative. Tali garanzie alternative devono essere sostanzialmente equivalenti a quelle richieste dall'articolo 47 della Carta dei diritti fondamentali dell'Unione europea (Carta dell'UE)[24].

53. In tal caso, l'accordo internazionale potrebbe creare una struttura che consenta all'interessato di far valere i propri diritti al di fuori degli organi giurisdizionali, ad esempio attraverso meccanismi para-giudiziari e vincolanti come l'arbitrato o meccanismi alternativi di risoluzione delle controversie come la mediazione, tali da garantire un controllo indipendente e da vincolare l'organismo pubblico destinatario[25]. Inoltre l'organismo pubblico che trasferisce i dati personali potrebbe impegnarsi a rispondere del risarcimento dei danni rilevati dal meccanismo di controllo indipendente in caso di trattamento illecito dei dati personali.

    In via eccezionale, l'accordo potrebbe prevedere altri meccanismi di ricorso ugualmente indipendenti ed efficaci, ad esempio meccanismi di questo tipo implementati da organizzazioni internazionali.

54. Con riguardo a tutti i meccanismi di ricorso sopra menzionati, l'accordo internazionale dovrebbe contenere l'obbligo per le parti di informarsi reciprocamente sull'esito del procedimento, in particolare se il reclamo dell'interessato è archiviato o non perviene a risoluzione.

55. L'esistenza di un meccanismo di ricorso deve associarsi alla possibilità per

l'organismo pubblico trasferente di sospendere o terminare il trasferimento di dati personali ai sensi dell'accordo internazionale, se le parti non riescono a risolvere la controversia in via amichevole, finché non ritenga che la questione sia stata affrontata in modo soddisfacente dall'organismo pubblico destinatario. Tale sospensione o cessazione, se effettuata, deve essere accompagnata dall'impegno dell'organismo pubblico destinatario a restituire o cancellare i dati personali. L'organismo pubblico trasferente deve notificare la sospensione o la cessazione all'autorità di controllo nazionale competente.

2.8 MECCANISMI DI CONTROLLO

56. Al fine di garantire il rispetto di tutti gli obblighi previsti dall'accordo internazionale, quest'ultimo deve prevedere un controllo indipendente della corretta applicazione dell'accordo, e delle ingerenze nei diritti previsti dall'accordo.

57. In primo luogo, l'accordo dovrebbe prevedere un meccanismo di controllo interno che ne garantisca il rispetto. Ciascuna parte dell'accordo dovrebbe condurre controlli interni periodici delle procedure messe in atto e dell'effettiva applicazione delle garanzie previste. I controlli interni periodici dovrebbero altresì verificare eventuali modifiche della legislazione che impedirebbero alle parti di rispettare i principi e le garanzie di protezione dei dati inclusi nell'accordo internazionale. Inoltre si potrebbe prevedere che una parte possa chiedere a un'altra parte dell'accordo di condurre tale riesame. L'accordo internazionale deve fare obbligo alle parti di rispondere alle richieste di una parte in merito all'effettiva attuazione delle garanzie in esso previste. Ciascuna parte che conduce un riesame dovrebbe comunicare i risultati dei controlli alle altre parti dell'accordo. Idealmente, tale comunicazione dovrebbe essere effettuata anche al meccanismo di controllo indipendente che vigila sull'accordo.

58. Inoltre l'accordo internazionale deve includere l'obbligo per una parte di informare l'altra parte senza indugio se per qualsiasi motivo non è in grado di dare efficace attuazione alle garanzie previste. In questo caso, l'accordo internazionale deve prevedere la possibilità per l'organismo pubblico trasferente di sospendere o terminare il trasferimento di dati personali all'organismo pubblico destinatario fino a quando quest'ultimo non informi l'organismo pubblico trasferente di essere nuovamente in grado di agire coerentemente con le garanzie. L'organismo trasferente deve notificare alla competente autorità di controllo nazionale le mutate circostanze nonché la sospensione dei trasferimenti o la risoluzione dell'accordo.

59. In secondo luogo, l'accordo deve prevedere un meccanismo di controllo indipendente incaricato di garantire che le parti ne rispettino le disposizioni. Tale previsione scaturisce direttamente dalla Carta dell'UE e dalla Convenzione europea dei diritti dell'uomo (CEDU)[27] in conformità della giurisprudenza della Corte europea dei diritti dell'uomo e di quanto stabilito nel diritto primario[28] nonché alla luce della pertinente giurisprudenza.

60. La Corte di giustizia dell'Unione europea, dal 2015[29], ribadisce la necessità di

disporre di un meccanismo di ricorso e controllo indipendente[30]. Allo stesso modo, la Corte europea dei diritti dell'uomo ha spesso sottolineato, nelle sue sentenze, che qualsiasi ingerenza nel diritto al rispetto della vita privata sancito dall'articolo 8 della CEDU deve essere soggetta a un sistema di controllo efficace, indipendente e imparziale[31].

61. L'accordo potrebbe, ad esempio, rinviare al controllo da parte di un'autorità di controllo competente, se presente nel paese dell'organismo pubblico che riceve i dati personali del SEE, anche se il GDPR non specifica che l'autorità di controllo competente debba essere un organismo di controllo esterno. Inoltre l'accordo potrebbe prevedere l'impegno della parte destinataria a cooperare su base volontaria con le autorità di controllo del SEE.

62. In assenza di un'autorità specificamente incaricata del controllo della normativa sulla protezione dei dati nel paese terzo o presso l'organizzazione internazionale, la necessità di un meccanismo di controllo e vigilanza indipendente, efficace e imparziale deve essere soddisfatta con altri mezzi. Il meccanismo di controllo indipendente messo in atto può dipendere dal caso specifico.

63. L'accordo potrebbe, ad esempio, fare riferimento a organismi di controllo esistenti nel paese terzo diversi da un'autorità di controllo nel settore della protezione dei dati. Inoltre, se non è possibile garantire un controllo esterno indipendente da un punto di vista strutturale o istituzionale, ad esempio a causa dei privilegi e delle immunità di alcune organizzazioni internazionali, il controllo potrebbe essere garantito attraverso meccanismi caratterizzati da autonomia funzionale. In quest'ultimo caso deve trattarsi di un organismo che, pur non essendo di per sé esterno all'ente, svolga le proprie funzioni in modo indipendente, ossia senza essere soggetto a istruzioni, con sufficienti risorse umane, tecniche e finanziarie, ecc. La parte destinataria è vincolata dalle decisioni dell'organismo di controllo.

2.9 CLAUSOLA DI RISOLUZIONE

64. L'accordo internazionale dovrebbe prevedere che tutti i dati personali trasferiti dal SEE ai sensi dell'accordo stesso prima della sua effettiva risoluzione continueranno ad essere trattati in conformità delle sue disposizioni.

INFORMAZIONI SPECIFICHE SULL'ARTICOLO 46 DEL GDPR

3.1 INFORMAZIONI SPECIFICHE SUGLI STRUMENTI GIURIDICAMENTE VINCOLANTI E AVENTI EFFICACIA ESECUTIVA

- ARTICOLO 46, PARAGRAFO 2, LETTERA A), DEL GDPR

65. L'articolo 46, paragrafo 2, lettera a), del GDPR consente agli organismi pubblici del SEE di fondare i trasferimenti a organismi pubblici in un paese terzo o ad un'organizzazione internazionale su strumenti pattizi che non necessitano dell'autorizzazione preventiva di un'autorità di controllo. Tali strumenti devono essere giuridicamente vincolanti e avere efficacia esecutiva. Pertanto, ai sensi di tale disposizione, possono essere utilizzati trattati internazionali, trattati di diritto pubblico o accordi amministrativi direttamente applicabili.
66. Qualsiasi strumento giuridicamente vincolante e avente efficacia esecutiva dovrebbe comprendere i principi fondamentali di protezione dei dati e i diritti degli interessati come richiesto dal GDPR.
67. Alle parti è fatto obbligo di impegnarsi a mettere in atto sufficienti garanzie di protezione dei dati per il trasferimento degli stessi. Di conseguenza, l'accordo dovrebbe stabilire anche in che modo l'organismo pubblico destinatario applicherà i principi fondamentali di protezione dei dati e i diritti degli interessati con riguardo a tutti i dati personali trasferiti, al fine di garantire che non sia compromesso il livello di protezione delle persone fisiche ai sensi del GDPR.
68. Se non è possibile garantire un ricorso giurisdizionale effettivo con strumenti giuridicamente vincolanti ed aventi efficacia esecutiva ed è pertanto necessario concordare un meccanismo di ricorso alternativo, gli organismi pubblici del SEE dovrebbero consultare l'autorità di controllo competente prima di definire tali strumenti.
69. Benché la forma dello strumento non sia decisiva nella misura in cui si tratti di uno strumento giuridicamente vincolante e dotato di efficacia esecutiva, l'EDPB ritiene che l'opzione migliore sarebbe quella di incorporare nello strumento stesso clausole dettagliate sulla protezione dei dati. Se tuttavia questa strada non è percorribile in ragione delle specifiche circostanze, l'EDPB raccomanda vivamente di incorporare direttamente nel testo dello strumento almeno una clausola generale che stabilisca i principi di protezione dei dati, e di inserire le disposizioni e garanzie più dettagliate in un allegato.

3.2 INFORMAZIONI SPECIFICHE SUGLI ACCORDI AMMINISTRATIVI - [ARTICOLO 46, PARAGRAFO 3, LETTERA B), DEL GDPR]

70. Anche l'articolo 46, paragrafo 3, lettera b), del GDPR prevede strumenti alternativi sotto forma di accordi amministrativi, ad esempio un protocollo d'intesa, in grado di fornire protezione attraverso gli impegni assunti da en-

trambe le parti per dare esecuzione all'accordo.

71. A tale riguardo, l'articolo 46, paragrafo 1, e il considerando 108 del GDPR specificano che tali accordi devono garantire all'interessato diritti azionabili e mezzi di ricorso effettivi. Laddove siano previste garanzie in accordi amministrativi che non sono giuridicamente vincolanti, è necessario ottenere l'autorizzazione dell'autorità di controllo competente.

72. Si dovrebbe valutare attentamente se ricorrere o meno ad accordi amministrativi non giuridicamente vincolanti per fornire garanzie nel settore pubblico, in considerazione delle finalità del trattamento e della natura dei dati in questione. Se il diritto interno del paese terzo o le norme interne/il quadro normativo dell'organizzazione internazionale non prevedono diritti di protezione dei dati né mezzi di ricorso per le persone fisiche del SEE, si dovrebbe privilegiare la conclusione di un accordo giuridicamente vincolante. Qualunque sia lo strumento adottato, le misure in vigore devono essere efficaci per garantire un'attuazione, un'applicazione e un controllo adeguati.

73. Negli accordi amministrativi devono essere adottate misure specifiche per garantire diritti azionabili alle persone nonché mezzi di ricorso e meccanismi di controllo effettivi. In particolare, per garantire diritti effettivi e azionabili, l'organismo pubblico che riceve i dati personali del SEE dovrebbe garantire, nello strumento non vincolante, che i diritti individuali siano pienamente garantiti dalla sua legislazione nazionale e possano essere esercitati dalle persone fisiche del SEE alle stesse condizioni dei cittadini e dei residenti del paese terzo interessato. Ciò vale anche qualora per le persone fisiche del SEE sia disponibile un mezzo di ricorso amministrativo e giudiziario in base al diritto interno del Paese dell'organismo pubblico destinatario. Allo stesso modo, le organizzazioni internazionali dovrebbero fornire garanzie sui diritti individuali previsti dalle loro norme interne, nonché sui meccanismi di ricorso disponibili.

74. Se ciò non fosse possibile, i diritti delle persone dovrebbero essere garantiti da impegni specifici assunti dalle parti, unitamente a meccanismi procedurali finalizzati ad assicurarne l'efficacia e a fornire un mezzo di ricorso alle persone. Tali specifici impegni e meccanismi procedurali devono consentire, nella pratica, di garantire il rispetto di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE dal GDPR.

75. I suddetti meccanismi procedurali possono, ad esempio, prevedere l'impegno delle parti a informarsi reciprocamente delle richieste dei cittadini del SEE e a risolvere le controversie o i reclami in modo tempestivo[32].

76. Inoltre, nel caso in cui tali controversie o reclami non possano essere risolti in via amichevole tra le parti, le persone devono avere la possibilità di proporre un ricorso indipendente ed effettivo attraverso meccanismi alternativi, ad esempio attraverso un meccanismo alternativo di risoluzione delle controversie, come l'arbitrato o la mediazione. Tale meccanismo alternativo di risoluzione delle controversie deve essere vincolante.

77. A seconda del caso specifico, l'accordo amministrativo dovrebbe prevedere tutte o alcune delle misure di cui sopra al fine di garantire un ricorso effetti-

vo. Potrebbero essere accettabili altre misure non menzionate nelle presenti linee guida purché prevedano un meccanismo di ricorso indipendente ed effettivo.

78. Ciascun accordo amministrativo concluso in conformità dell'articolo 46, paragrafo 3, lettera b), del GDPR sarà esaminato dall'autorità di controllo competente guardando alle specifiche circostanze, e a tale esame farà seguito la relativa procedura dell'EDPB, se applicabile. L'autorità di controllo competente informerà la propria valutazione alle raccomandazioni generali contenute nelle presenti linee guida, ma potrebbe anche chiedere maggiori garanzie a seconda del caso specifico.

4. QUESTIONI PROCEDURALI

Gli accordi amministrativi stabiliti ai sensi dell'articolo 46, paragrafo 3, lettera b), del GDPR saranno esaminati caso per caso tenuto conto della necessità di un'autorizzazione da parte dell'autorità di controllo competente che, ai sensi dell'articolo 46, paragrafo 4, del GDPR, applica il meccanismo di coerenza ai sensi dell'articolo 64, paragrafo 2, del GDPR. Nell'integrare meccanismi di ricorso alternativi in strumenti vincolanti ed aventi efficacia esecutiva ai sensi dell'articolo 46, paragrafo 2, lettera a), del GDPR, l'EDPB raccomanda di consultare anche l'autorità di controllo competente. L'EDPB consiglia vivamente di consultare tempestivamente l'autorità di controllo competente.

Per il Comitato europeo per la protezione dei dati
La presidente

(Andrea Jelinek)

NOTE

[1] Nelle presenti linee guida, i riferimenti agli "Stati membri" sono da intendersi come riferimenti agli "Stati membri del SEE".

[2] Ad esempio gli organismi pubblici giapponesi, che non rientrano nell'ambito di applicazione della decisione di adeguatezza relativa al Giappone in quanto quest'ultima riguarda solo le organizzazioni del settore privato.

[3] Le presenti linee guida utilizzano l'espressione "accordi internazionali" per fare riferimento a strumenti giuridicamente vincolanti e aventi efficacia esecutiva ai sensi dell'articolo 46, paragrafo 2, lettera a), del GDPR e agli accordi amministrativi ai sensi dell'articolo 46, paragrafo 3, lettera b), del GDPR.

[4] L'articolo 96 del GDPR stabilisce che gli accordi conclusi prima del 24 maggio 2016 restano in vigore fino alla loro modifica, sostituzione o revoca.

[5] Il gruppo di lavoro delle autorità dell'UE per la protezione dei dati istituito ai sensi dell'articolo 29 della direttiva 95/46/CE sulla protezione dei dati.

[6] Cfr. gruppo di lavoro "Articolo 29", Criteri di riferimento per l'adeguatezza (WP254 rev. 01, approvato dall'EDPB il 25 maggio 2018), Linee guida EDPB 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679 e Linee guida EDPB 3/2018 sull'ambito di applicazione territoriale del RGPD (articolo 3).

[7] Direttiva (UE) 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

[8] Corte di giustizia dell'Unione europea, causa C-311/18, *Data Protection Commissioner/Facebook Ireland Limited e Maximillian Schrems* ("Schrems II", punto 96).

[9] Per ulteriori informazioni sull'articolo 49 e sulla sua interazione con l'articolo 46 in generale, consultare le linee guida EDPB 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679.

[10] Cfr. le linee guida EDPB 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679, pag. 11.

[11] Cfr. le linee guida EDPB sulle deroghe di cui all'articolo 49 del regolamento 2016/679, pag. 5.

[12] Cfr. anche il considerando 108 del GDPR.

[13] Cfr. ad esempio la definizione di "ente pubblico" e di "organismo di diritto pubblico" di cui all'articolo 2, paragrafi 1 e 2, della direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico (GU L 345 del 31.12.2003, pag. 90).

[14] Cfr. linee guida EDPB 3/2018 sull'ambito di applicazione territoriale del RGPD, pag. 25.

[15] L'articolo 44 del GDPR recita: "*Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato*".

[16] Corte di giustizia dell'Unione europea, sentenza del 16 luglio 2020 nella causa C-311/18, *Data Protection Commissioner/Facebook Ireland Limited e Maximillian Schrems* ("Schrems II").

[17] Corte di giustizia dell'Unione europea, sentenza del 16 luglio 2020 nella causa C-311/18, *Data Protection Commissioner/Facebook Ireland Limited e Maximillian Schrems* ("Schrems II", punto 105).

[18] Idem.

[19] Cfr. linee guida dell'EDPB sulla trasparenza ai sensi del regolamento 2016/679, WP 260, rev. 01, pagine da 13 a 23.

[20] Cfr. la sezione 2.3.1.

[21] Cfr. raccomandazioni EDPB 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza.

[22] Cfr. raccomandazioni EDPB 2/2020, garanzia D, pag. 13 e segg.

[23] Cfr. anche la sezione 2.8 sul meccanismo di controllo.

[24] Corte di giustizia dell'Unione europea, sentenza del 16 luglio 2020 nella causa C-311/18, *Data Protection Commissioner/Facebook Ireland Limited e Maximillian Schrems* ("Schrems II", punti 96, 186 e segg.).

[25] Corte di giustizia dell'Unione europea, sentenza del 6 ottobre 2015 nella causa C-362/14, *Maximillian Schrems/Data Protection Commissioner* ("Schrems", punti 41 e 95); Corte di giustizia dell'U-

nione europea, sentenza del 16 luglio 2020 nella causa C-311/18, *Data Protection Commissioner/ Facebook Ireland Limited e Maximillian Schrems* ("Schrems II", punti 186, 187, 189, 195 e segg.).

[26] Articoli 7, 8 e 47 della Carta dell'UE.

[27] Articolo 8 della CEDU.

[28] Articolo 6 del trattato di Lisbona
"*1. L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati.*
Le disposizioni della Carta non estendono in alcun modo le competenze dell'Unione definite nei trattati.
I diritti, le libertà e i principi della Carta sono interpretati in conformità delle disposizioni generali del titolo VII della Carta che disciplinano la sua interpretazione e applicazione e tenendo in debito conto le spiegazioni cui si fa riferimento nella Carta, che indicano le fonti di tali disposizioni.
2. L'Unione aderisce alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Tale adesione non modifica le competenze dell'Unione definite nei trattati.
3. I diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali".

[29] Corte di giustizia dell'Unione europea, sentenza del 6 ottobre 2015 nella causa C-362/14, *Maximillian Schrems/Data Protection Commissioner* ("Schrems", punti 41 e 95).

[30] Corte di giustizia dell'Unione europea, 27 luglio 2017, parere 1/15 sull'accordo sul trasferimento dei dati del codice di prenotazione, previsto tra l'Unione europea e il Canada, 26 luglio 2017 (punti 228 e segg.); Corte di giustizia dell'Unione europea, 30 aprile 2019, parere 1/17 sull'accordo economico e commerciale globale tra il Canada e l'Unione europea (punti 190 e segg.).

[31] Corte europea dei diritti dell'uomo, 6 settembre 1978, Klass contro Germania (punti 55 e 56). Il requisito derivante dalla Corte europea dei diritti dell'uomo si applica anche a qualsiasi ingerenza negli articoli 7 e 8 della Carta dell'UE poiché, ai sensi dell'articolo 52, paragrafo 3, della Carta dell'UE, il significato e l'ambito di applicazione di tali diritti fondamentali sono uguali a quelli stabiliti dall'articolo 8 della CEDU.

[32] Corte di giustizia dell'Unione europea, sentenza del 16 luglio 2020 nella causa C-311/18, *Data Protection Commissioner/Facebook Ireland Limited e Maximillian Schrems* ("Schrems II", punti 189, 196 e segg.).

Linee guida 4/2021 sui codici di condotta come strumento per i trasferimenti Versione 2.0

Adottate il 22 febbraio 2022

Cronologia delle versioni

Versione 2.0	22 febbraio 2022	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	7 luglio 2021	Adozione delle linee guida per la consultazione pubblica

SINTESI

L'articolo 46 del regolamento generale sulla protezione dei dati (di seguito "GDPR") sancisce che i titolari/responsabili del trattamento predispongano garanzie adeguate per i trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali. A tal fine, il GDPR diversifica le garanzie adeguate che possono essere utilizzate dalle organizzazioni a norma dell'articolo 46 per inquadrare i trasferimenti verso paesi terzi, introducendo, tra l'altro, i codici di condotta come nuovo meccanismo per i trasferimenti (articolo 40, paragrafo 3, e articolo 46, paragrafo 2, lettera e)). A questo proposito, come previsto dall'articolo 40, paragrafo 3, a un codice di condotta che è stato approvato dall'autorità di controllo competente e di cui la Commissione ha riconosciuto la validità generale all'interno dell'Unione possono aderire, e utilizzarlo, i titolari o i responsabili del trattamento non soggetti al GDPR situati in paesi terzi allo scopo di fornire garanzie adeguate ai dati trasferiti verso tali paesi. Detti titolari o responsabili del trattamento sono tenuti ad assumere impegni vincolanti e azionabili, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie fornite dal codice anche per quanto riguarda i diritti degli interessati, conformemente a quanto disposto dall'articolo 40, paragrafo 3. Le linee guida individuano elementi che dovrebbero figurare in tali impegni.

Occorre rilevare inoltre che un codice destinato ai trasferimenti a cui ha aderito un importatore di dati in un paese terzo può essere utilizzato dai titolari/responsabili del trattamento soggetti al GDPR (vale a dire gli esportatori di dati) per adempiere ai loro obblighi in caso di trasferimenti verso paesi terzi conformemente al GDPR, senza la necessità di aderire essi stessi a tale codice.

In termini di contenuto, un codice destinato ai trasferimenti e volto a fornire garanzie adeguate a norma dell'articolo 46 dovrebbe contemplare i principi essenziali, i diritti e gli obblighi derivanti dal GDPR per i titolari/responsabili del trattamento nonché le garanzie specifiche con riguardo al contesto dei trasferimenti (ad esempio per quanto riguarda i trasferimenti successivi o legislazione confliggente nel paese terzo). Alla luce delle garanzie fornite a norma dell'articolo 46 del GDPR dagli strumenti per i trasferimenti esistenti, e per assicurare la coerenza nel livello di protezione, nonché tenuto conto della sentenza Schrems II della Corte di giustizia dell'Unione europea[1], le linee guida forniscono una lista di controllo degli elementi che devono figurare in un codice di condotta destinato ai trasferimenti.

Un codice di condotta può essere redatto inizialmente al solo scopo di precisare l'applicazione del GDPR a norma dell'articolo 40, paragrafo 2 ("codice sul GDPR") oppure anche nell'ottica di un codice destinato ai trasferimenti conformemente all'articolo 40, paragrafo 3. Di conseguenza, a seconda dello scopo e del contenuto iniziale del codice, potrebbe essere necessario apportare modifiche per ricomprendervi tutti gli elementi di cui sopra, se si intende utilizzarlo come strumento per i trasferimenti.

Le presenti linee guida, che integrano le linee guida del Comitato europeo per la protezione dei dati (in appresso: "'EDPB") 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento 2016/679, forniscono chiarimenti, attraverso diagrammi di flusso, per quanto riguarda il ruolo dei diversi attori coinvolti nella definizione di un codice da utilizzare come strumento per i trasferimenti e il relativo processo di adozione.

Indice

1 Ambito di applicazione delle linee guida

2 Cosa sono i codici di condotta come strumento per i trasferimenti?

3 Quale dovrebbe essere il contenuto di un codice di condotta come strumento per i trasferimenti?

4 Chi sono i soggetti coinvolti nella creazione di un codice da utilizzare come strumento per i trasferimenti e qual è il loro ruolo?
- 4.1 Titolare del codice
- 4.2 Organismo di monitoraggio
- 4.3 Autorità di controllo
- 4.4 Comitato europeo per la protezione dei dati
- 4.5 Commissione

5 Processo di adozione di un codice di condotta per i trasferimenti

6 Quali sono le garanzie da fornire nell'ambito del codice?
- 6.1 Impegni vincolanti e azionabili da attuare
- 6.2 Lista di controllo degli elementi da includere in un codice di condotta destinato ai trasferimenti

Allegato 1 - Adozione di un codice di condotta per i trasferimenti - Diagramma di flusso
- a - Adozione di un codice transnazionale destinato ai trasferimenti
- b - Modifiche a un codice transnazionale da utilizzare come codice destinato ai trasferimenti

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018[2],

visti gli articoli 12 e 22 del proprio regolamento interno,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

1. AMBITO DI APPLICAZIONE DELLE LINEE GUIDA

1. Lo scopo delle presenti linee guida è precisare l'applicazione dell'articolo 40, paragrafo 3, del GDPR, relativo ai codici di condotta come garanzie adeguate per i trasferimenti di dati personali verso paesi terzi, conformemente all'articolo 46, paragrafo 2, lettera e), del GDPR. Esse mirano inoltre a fornire una guida pratica, anche per quanto riguarda il contenuto di tali codici di condotta, il loro processo di adozione e i soggetti coinvolti, nonché i requisiti che un codice di condotta per i trasferimenti deve soddisfare e le garanzie che deve fornire.
2. Le presenti linee guida intendono altresì offrire un riferimento univoco per tutte le autorità di controllo e il Comitato, e dovrebbero assistere la Commissione europea ("la Commissione") nella valutazione coerente dei codici snellendo le procedure previste nel processo di valutazione. Un ulteriore obiettivo perseguito è favorire la trasparenza, assicurando che i titolari dei codici che intendono chiedere l'approvazione di un codice di condotta destinato a essere utilizzato come strumento per i trasferimenti ("codice destinato ai trasferimenti") siano pienamente consapevoli del processo e comprendano i requisiti formali e i presupposti per la definizione diun codice di condotta di tal genere.
3. Le presenti linee guida integrano le linee guida dell'EDPB 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento 2016/679, che istituiscono il quadro generale per l'adozione di codici di condotta ("linee guida 1/2019"). Le considerazioni esposte nelle linee guida 1/2019, in particolare per quanto riguarda l'ammissibilità, la presentazione e i criteri di approvazione, sono quindi valide anche nel contesto dell'elaborazione dei codici destinati ai trasferimenti.

2. COSA SONO I CODICI DI CONDOTTA COME STRUMENTO PER I TRASFERIMENTI?

4. L'articolo 46 del GDPR impone ai titolari/responsabili del trattamento di fornire garanzie adeguate per i trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali.
5. A tal fine, il GDPR prevede varie tipologie di garanzie adeguate che possono essere utilizzate dalle organizzazioni a norma dell'articolo 46 per inquadrare i trasferimenti verso paesi terzi introducendo, tra l'altro, i codici di condotta come nuovo meccanismo per i trasferimenti (articolo 40, paragrafo 3 e articolo 46, paragrafo 2, lettera e). A questo proposito, come previsto dall'articolo 40, paragrafo 3, a un codice di condotta che è stato approvato dall'autorità di controllo competente e di cui la Commissione ha riconosciuto la validità generale all'interno dell'Unione possono aderire, e utilizzarlo, anche i titolari o i responsabili del trattamento non soggetti al GDPR situati in paesi terzi allo scopo di fornire garanzie adeguate ai dati trasferiti verso paesi terzi. Detti titolari o responsabili del trattamento sono tenuti ad assumere l'impegno

vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie fornite dal codice anche per quanto riguarda i diritti degli interessati, conformemente a quanto disposto dall'articolo 40, paragrafo 3.

6. I codici di condotta possono essere elaborati da associazioni o altri organismi che rappresentano categorie di titolari o responsabili del trattamento (titolari dei codici), come specificato dall'articolo 40, paragrafo 2. Come indicato nelle linee guida 1/2019, un elenco non esaustivo di possibili titolari di codici comprende associazioni di categoria e rappresentative, organismi di settore, organizzazioni accademiche e gruppi d'interesse. Secondo le stesse linee guida, i codici destinati ai trasferimenti potrebbero, ad esempio, essere elaborati da organismi che rappresentano un settore (ad esempio un'associazione/federazione del settore bancario e finanziario o del settore assicurativo) ma potrebbero anche essere elaborati per settori distinti che hanno un'attività di trattamento comune e condividono caratteristiche ed esigenze di trattamento (ad esempio un codice delle risorse umane elaborato da un'associazione/federazione di professionisti delle risorse umane, o un codice relativo al trattamento di dati dei minori). Tali codici consentirebbero pertanto ai titolari e ai responsabili del trattamento in paesi terzi, che ricevono dati a norma del codice, di disciplinare tali trasferimenti gestendo al contempo in modo migliore le esigenze di trattamento specifiche del proprio settore o le attività di trattamento comuni. Tali codici potrebbero quindi costituire uno strumento più idoneo rispetto ad altri meccanismi di trasferimento disponibili a norma dell'articolo 46. I codici di condotta da utilizzare come strumento per i trasferimenti consentiranno, in particolare, a un titolare o responsabile del trattamento in un paese terzo di fornire garanzie adeguate per molteplici trasferimenti verso tale paese terzo secondo modalità specifiche per il determinato settore o attività di trattamento. Inoltre non occorre che i soggetti aderenti a un codice di condotta appartengano a uno stesso gruppo (come è invece richiesto nel caso delle norme vincolanti d'impresa).

7. Occorre rilevare, inoltre, che un codice destinato ai trasferimenti a cui ha aderito un importatore di dati in un paese terzo può essere utilizzato dai titolari/responsabili del trattamento soggetti al GDPR (vale a dire gli esportatori di dati) per adempiere ai loro obblighi in caso di trasferimenti verso paesi terzi conformemente al GDPR, senza la necessità di aderire essi stessi a tale codice. Pertanto un codice destinato ai trasferimenti potrebbe disciplinare i trasferimenti da titolari/responsabili del trattamento che non aderiscono a tale codice di condotta verso titolari/responsabili del trattamento in un paese terzo che vi hanno aderito, a condizione che uno strumento vincolante preveda l'impegno a rispettare gli obblighi stabiliti dal codice di condotta relativamente al trattamento dei dati trasferiti, anche, in particolare, per quanto riguarda i diritti degli interessati. Ciò significa che l'importatore di dati nel paese terzo deve aderire al codice destinato ai trasferimenti mentre gli esportatori di dati soggetti al GDPR non devono necessariamente aderirvi. Anche i gruppi di imprese che trasferiscono dati da soggetti cui si applica il GDPR ad altri soggetti posti al di fuori del SEE possono utilizzare un codice di condotta come strumento per i trasferimenti se le imprese del gruppo situa-

te al di fuori del SEE hanno aderito a tale codice per i trasferimenti e hanno assunto impegni vincolanti e azionabili con riguardo a tali trasferimenti.

Esempio 1[3]

la società XYZ ha sede in Italia e ha filiali in Germania, Olanda, Spagna e Belgio. Allo scopo di gestire gli strumenti informatici utilizzati dal gruppo, la società XYZ ricorre alle prestazioni di un fornitore di servizi cloud con sede in un paese terzo senza presenza nell'UE. Il trattamento dei dati nell'ambito dell'utilizzo di strumenti informatici comporta trasferimenti di dati dalla società XYZ e dalle sue affiliate al fornitore di servizi cloud allo scopo di memorizzarli. Poiché il fornitore di servizi cloud nel paese terzo ha aderito a un codice di condotta destinato ai trasferimenti in relazione ai servizi cloud, approvato a norma dell'articolo 40, paragrafo 5, i flussi di dati dalla società XYZ e dalle sue affiliate al fornitore di servizi cloud possono essere disciplinati attraverso il codice di condotta a cui quest'ultimo ha aderito. In questo caso, l'utilizzo di un codice di condotta da parte del fornitore di servizi cloud invece di altri strumenti di trasferimento, come le norme vincolanti d'impresa, sembra più appropriato in quanto un codice di condotta non impone al titolare /responsabile del trattamento che agisce da importatore di avere una presenza nel SEE, mentre tale presenza è richiesta nel caso di un gruppo di società che utilizzi norme vincolanti d'impresa. Il codice di condotta presenta anche ulteriori vantaggi in quanto consente molteplici trasferimenti di dati con un unico strumento rispetto a soluzioni (completamente) contrattuali come le clausole contrattuali tipo.

8. Un codice destinato ai trasferimenti potrebbe anche servire a disciplinare i trasferimenti da titolari/responsabili del trattamento soggetti al GDPR a titolari/responsabili del trattamento in un paese terzo che abbiano aderito allo stesso codice di condotta per i trasferimenti, sempre che, come spiegato sopra, uno strumento vincolante preveda l'impegno a rispettare gli obblighi del codice di condotta anche con riguardo ai diritti degli interessati sanciti dal GDPR.

Esempio 2

un'associazione che rappresenta categorie di titolari/responsabili del trattamento coinvolti nello stesso tipo di attività di ricerca per il settore sanitario che comportano trasferimenti regolari di dati a titolari e responsabili del trattamento di paesi terzi, elabora un codice di condotta destinato a essere utilizzato anche come strumento per i trasferimenti. I titolari/responsabili del trattamento nel SEE aderiscono a questo codice di condotta a cui hanno aderito anche i titolari/responsabili del trattamento dei paesi terzi. I trasferimenti di dati a titolari/responsabili del trattamento dei paesi terzi nel contesto delle attività di ricerca possono essere disciplinati ai sensi di tale codice di condotta.

9. Nella misura in cui è molto probabile che i codici destinati ai trasferimenti siano utilizzati per disciplinare i trasferimenti da più di uno Stato membro, e considerando che tali codici di condotta dovrebbero avere validità generale a norma dell'articolo 40, paragrafo 9, del GDPR, essi si configurerebbero quindi come "codici transnazionali" secondo quanto definito nelle linee guida 1/2019[4].

3. QUALE DOVREBBE ESSERE IL CONTENUTO DI UN CODICE DI CONDOTTA COME STRUMENTO PER I TRASFERIMENTI?

10. Come indicato sopra, un codice di condotta destinato ai trasferimenti è uno degli strumenti che possono essere utilizzati dalle organizzazioni che svolgono particolari attività di trattamento dei dati, ad esempio all'interno di un settore specifico, o un'attività di trattamento comune, che condividono le stesse caratteristiche ed esigenze di trattamento, per fornire garanzie adeguate ai fini dei trasferimenti di dati personali verso un paese terzo conformemente all'articolo 46.
11. Inoltre le disposizioni dell'articolo 40, paragrafo 3, in base alle quali ai codici destinati ai trasferimenti possono aderire titolari/responsabili del trattamento non soggetti al GDPR a norma dell'articolo 3, lasciano intendere che tali codici sono, in misura parziale o totale, concepiti più specificamente per i titolari/responsabili del trattamento situati in paesi terzi. Pertanto, l'EDPB ritiene che un codice destinato ai trasferimenti dovrebbe stabilire anche le norme che dovranno essere rispettate dal titolare/responsabile del trattamento del paese terzo (l'importatore di dati) al fine di garantire che i dati personali siano adeguatamente protetti in linea con i requisiti del capo V del GDPR quando sono trattati da tale titolare/responsabile del trattamento (vale a dire dall'importatore di dati) nel paese terzo.
12. Più specificamente, in termini di contenuto, affinché siano fornite garanzie adeguate a norma dell'articolo 46, il codice di condotta deve contemplare gli elementi seguenti:

- principi essenziali, diritti e obblighi derivanti dal GDPR per i titolari/responsabili del trattamento; e
- garanzie specifiche con riguardo al contesto dei trasferimenti (ad esempio per quanto concerne la questione dei trasferimenti successivi o l'esistenza di legislazione confliggente nel paese terzo).

13. A questo proposito, è opportuno osservare che un codice di condotta può essere redatto inizialmente al solo scopo di precisare l'applicazione del GDPR a norma dell'articolo 40, paragrafo 2 ("codice GDPR") ovvero anche come codice destinato ai trasferimenti conformemente all'articolo 40, paragrafo 3. Di conseguenza, a seconda dello scopo e del contenuto iniziale del codice, potrebbe essere necessario apportarvi modifiche per ricomprendere tutti gli elementi di cui sopra, ove si intenda utilizzarlo come strumento per i trasferimenti.

Esempio 3

l'associazione ABC, alla quale aderiscono organizzazioni che operano nel settore del marketing diretto nell'UE, ha adottato un codice di condotta che mira a specificare l'applicazione del principio di trasparenza e dei relativi requisiti a norma del GDPR nell'ambito delle attività di trattamento per tale settore. L'associazione desidera utilizzare tale codice di condotta come strumento per disciplinare i trasferimenti al di fuori del SEE. Poiché il codice di condotta si concentra sul principio di trasparenza, per ottenere l'approvazione come codice destinato ai trasferimenti esso dovrebbe essere modificato per includervi anche le garanzie adeguate necessarie per i trasferimenti internazionali di dati personali, tutti i principi essenziali e i requisiti principali derivanti dal GDPR (diversi dalla trasparenza), nonché garanzie specifiche rispetto al contesto dei trasferimenti.

14. In ogni caso, conformemente con i chiarimenti forniti dall'EDPB nelle linee guida 1/2019, il codice dovrà esplicitare tutti gli elementi atti a fornire garanzie adeguate di cui sopra in modo tale da facilitarne l'effettiva applicazione e precisarne l'applicazione pratica allo specifico settore o attività di trattamento[5].

15. La sezione 6 delle presenti linee guida contiene una descrizione ragionata sotto forma di lista di controllo degli elementi da includere in un codice destinato ai trasferimenti affinché si possa ritenere che tale codice fornisca garanzie adeguate.

4. CHI SONO I SOGGETTI COINVOLTI NELLA CREAZIONE DI UN CODICE DA UTILIZZARE COME STRUMENTO PER I TRASFERIMENTI E QUAL È IL LORO RUOLO?

4.1 TITOLARE DEL CODICE

16. Il titolare del codice è il soggetto, l'associazione, la federazione o altro organismo che elaborerà un codice di condotta destinato ai trasferimenti o modificherà un "codice GDPR" approvato per utilizzarlo come strumento per i trasferimenti e lo sottoporrà all'autorità di controllo competente per approvazione[6].

4.2 ORGANISMO DI MONITORAGGIO

17. Come per qualsiasi codice di condotta, dovrà essere individuato un organismo di monitoraggio specifico anche per il codice destinato ai trasferimenti, e tale organismo dovrà essere accreditato dall'autorità di controllo competente in linea con l'articolo 41. Più precisamente, il ruolo di tale organismo sarà quello di controllare che i titolari/responsabili del trattamento di paesi terzi che hanno aderito a tale codice si attengano alle norme in esso stabilite[7].

18. Considerato che i codici di condotta destinati ai trasferimenti sono anche, o più specificamente, rivolti ai titolari/responsabili del trattamento di pae-

si terzi, occorre assicurarsi che gli organismi di monitoraggio siano in grado di monitorare efficacemente il codice come specificato nelle linee guida 1/2019. Gli organismi di monitoraggio operanti nell'ambito dei codici destinati ai trasferimenti potrebbero avere la sede solo all'interno o anche al di fuori del SEE, purché abbiano uno stabilimento nel SEE. In questo contesto, lo stabilimento dell'organismo di monitoraggio nel SEE è quello della sua sede centrale o del luogo in cui vengono prese le decisioni finali riguardanti le attività di monitoraggio; inoltre, è necessario che lo stabilimento nel SEE sia in grado di controllare le sedi dell'organismo di monitoraggio al di fuori del SEE e di assumersi piena responsabilità per tutte le decisioni e azioni (compresa la responsabilità in caso di violazioni).

19. Inoltre un organismo di monitoraggio nel SEE può esternalizzare le attività a un diverso soggetto stabilito al di fuori del SEE e che agisce per suo conto, a condizione che tale soggetto disponga della stessa competenza e perizia richiesta dal codice di condotta e dai requisiti di accreditamento, e che l'organismo di monitoraggio nel SEE sia in grado di assicurare un controllo efficace sui servizi forniti dall'appaltatore e mantenga il potere decisionale sulle attività di monitoraggio. Per garantire il rispetto di tali requisiti di accreditamento nell'esternalizzazione di parte dei propri compiti, l'organismo di monitoraggio deve stipulare un contratto o un altro atto giuridico a norma del diritto dell'Unione che vincoli l'appaltatore nei propri confronti, in modo tale che tutte le attività esternalizzate soddisfino i requisiti del GDPR. L'esternalizzazione non comporta la delega di responsabilità: in ogni caso, l'organismo di monitoraggio rimane responsabile del monitoraggio del rispetto del codice di condotta nei confronti dell'autorità di controllo. L'organismo di monitoraggio assicura che tutti gli appaltatori soddisfino i requisiti stabiliti dal suddetto documento sui requisiti di accreditamento, in particolare per quanto riguarda l'indipendenza, l'assenza di conflitti d'interesse e la competenza. L'organismo di monitoraggio include una clausola specifica nel contratto firmato con gli appaltatori per garantire la riservatezza dei dati personali che possono eventualmente essere comunicati durante le attività di monitoraggio e prevede garanzie adeguate in caso di trasferimento di tali dati personali ai propri appaltatori.

4.3 AUTORITÀ DI CONTROLLO

20. Conformemente all'articolo 40, paragrafo 5, il ruolo dell'autorità di controllo competente sarà quello di approvare il progetto di codice di condotta destinato ai trasferimenti, o le modifiche apportate a un codice esistente per utilizzarlo come strumento per i trasferimenti, e di accreditare l'organismo di monitoraggio individuato nell'ambito del codice rispetto ai requisiti di accreditamento specifici dei codici destinati ai trasferimenti.

4.4 COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

21. A norma dell'articolo 40, paragrafo 7 e dell'articolo 64, paragrafo 1, lettera b, all'EDPB sarà chiesto di fornire un parere sul progetto di decisione di un'autorità di controllo che mira ad approvare un codice destinato ai trasferimenti o una modifica a un codice di condotta per utilizzarlo anche come strumento per i trasferimenti[8].

4.5 COMMISSIONE

22. Come previsto dall'articolo 40, paragrafo 9, la Commissione può decidere, mediante un atto di esecuzione, che un codice destinato ai trasferimenti approvato da un'autorità di controllo ha validità generale all'interno dell'Unione. Solo i codici ai quali è stata concessa validità generale all'interno dell'Unione possono essere invocati per inquadrare i trasferimenti.

5. PROCESSO DI ADOZIONE DI UN CODICE DI CONDOTTA PER I TRASFERIMENTI

23. Dall'articolo 40, paragrafi 5 e 9, si evince che ai fini dell'adozione di un codice destinato ai trasferimenti sono necessari la previa approvazione di un'autorità di controllo competente nel SEE e il successivo riconoscimento da parte della Commissione europea, mediante un atto di esecuzione, della validità generale di tale codice all'interno dell'Unione.
24. Come menzionato nella sezione 2, poiché è assai probabile che i codici destinati ai trasferimenti siano utilizzati dai titolari/responsabili del trattamento per disciplinare i trasferimenti da più di uno Stato membro, si tratterà verosimilmente di "codici transnazionali" soggetti alla procedura di approvazione, come specificata nella sezione 8 e nell'allegato 4 delle linee guida 1/2019[9], compresa la necessità di un parere dell'EDPB. In pratica possono presentarsi diversi scenari quando un'associazione/federazione o un altro organismo intende adottare un codice di condotta per i trasferimenti:

- un progetto di codice è concepito sia come "codice GDPR" che come strumento per i trasferimenti utilizzabile da parte di titolari/responsabili del trattamento di paesi terzi. Tale progetto di codice dovrebbe prima essere approvato dall'autorità di controllo competente secondo la procedura per i codici transnazionali, che prevede il parere del Comitato, e poi riconosciuto dalla Commissione come avente validità generale all'interno dell'Unione conformemente all'articolo 40, paragrafo 9. Dopo aver completato questi passaggi, i titolari/responsabili del trattamento nei paesi terzi possono aderire al codice e quest'ultimo può essere utilizzato al fine di fornire garanzie adeguate per i trasferimenti di dati verso paesi terzi;
- inizialmente un codice di condotta è concepito e approvato come "codice GDPR". Tale codice viene ulteriormente ampliato per essere utilizzabile anche da parte di titolari/responsabili del trattamento di paesi terzi come stru-

mento per i trasferimenti. La modifica del codice relativa ai trasferimenti dovrà essere presentata all'autorità di controllo competente per approvazione, sulla base della procedura per i codici transnazionali che prevede il parere del Comitato. Il codice una volta modificato dovrà poi essere riconosciuto dalla Commissione come avente validità generale all'interno dell'Unione a norma dell'articolo 40, paragrafo 9; dopodiché i titolari/responsabili del trattamento nei paesi terzi potranno aderire a tale codice e utilizzarlo al fine di fornire garanzie adeguate per i trasferimenti di dati personali verso paesi terzi.

25. Un diagramma di flusso riportato nell'allegato alle linee guida illustra nel dettaglio la procedura prevista per l'adozione di un codice di condotta destinato ai trasferimenti, alla luce degli scenari potenziali sopra descritti.

6. QUALI SONO LE GARANZIE DA FORNIRE NELL'AMBITO DEL CODICE?

6.1 IMPEGNI VINCOLANTI E AZIONABILI DA ATTUARE

26. L'articolo 40, paragrafo 3, del GDPR, impone ai titolari e ai responsabili del trattamento non soggetti al GDPR che aderiscono a un codice destinato ai trasferimenti di assumere l'impegno vincolante e azionabile, mediante strumenti contrattuali o altri strumenti giuridicamente vincolanti, di applicare le garanzie adeguate previste dal codice, in particolare per quanto riguarda i diritti degli interessati.

27. Come specificato dal GDPR, tali impegni possono essere assunti mediante la stipula di un contratto, che appare essere la soluzione più semplice. Si potrebbero usare anche altri strumenti, purché i titolari/responsabili del trattamento che aderiscono al codice siano in grado di dimostrare il carattere vincolante e azionabile di tali diversi strumenti.

28. In ogni caso, lo strumento dev'essere vincolante e azionabile, conformemente al diritto dell'Unione, e dev'essere vincolante e azionabile anche da parte degli interessati in quanto terzi beneficiari.

29. Gli aderenti a un codice di condotta come strumento per i trasferimenti possono essere stabiliti sia nel SEE sia al di fuori di esso. Una differenza significativa tra i primi e i secondi è data dalla diretta applicabilità del GDPR ai primi (stabiliti nel SEE) ma non ai secondi (sempre che questi ultimi non rientrino nel campo di applicazione dell'articolo 3, paragrafo 2, del GDPR).

30. Per quanto riguarda gli aderenti al codice stabiliti al di fuori del SEE, occorre assicurare che il loro impegno ad applicare un "determinato livello di protezione dei dati" garantisca il rispetto del livello di protezione dei dati previsto dal GDPR. Questo elemento è un prerequisito ai fini della loro idoneità ad aderire al codice di condotta come strumento di trasferimento.

31. A tal fine, il titolare/responsabile del trattamento nel paese terzo (vale a dire l'importatore di dati) potrebbe stipulare un contratto, ad esempio, con il soggetto che trasferisce i dati in virtù del codice (vale a dire l'esportatore di dati). In pratica, potrebbe utilizzare un contratto già esistente (ad esempio un ac-

cordo di servizio tra l'esportatore e l'importatore di dati o il contratto da predisporre a norma dell'articolo 28 del GDPR in caso di importatori-responsabili del trattamento), nel quale si potrebbero includere gli impegni vincolanti e azionabili. Un'altra soluzione potrebbe essere quella di affidarsi a un contratto distinto aggiungendo al codice destinato ai trasferimenti un contratto-tipo che dovrebbe essere poi firmato, ad esempio, dai titolari/responsabili del trattamento nel paese terzo e da tutti i rispettivi esportatori di dati.

32. Dovrebbe essere garantita una certa flessibilità nella scelta dell'opzione più adeguata a seconda della situazione specifica.

33. Qualora il codice di condotta debba essere utilizzato per i trasferimenti e i trasferimenti successivi da un responsabile del trattamento a sub-responsabili del trattamento, nell'accordo stipulato tra il responsabile del trattamento e il rispettivo titolare del trattamento occorre, se possibile, anche rinviare al codice di condotta e allo strumento che prevede impegni vincolanti e azionabili.

Impegni vincolanti e azionabili da parte dell'importatore di dati (esempio)

34. In generale, il contratto o altro strumento deve stabilire che il titolare/responsabile del trattamento si impegna a rispettare le norme specificate nel codice destinato ai trasferimenti nel trattamento dei dati ricevuti a norma del codice stesso. Il contratto o altro strumento deve altresì prevedere meccanismi che consentano di far rispettare tali impegni in caso di violazioni da parte del titolare/responsabile del trattamento, in particolare per quanto riguarda i diritti degli interessati i cui dati saranno trasferiti a norma del codice.

35. Più in particolare, il contratto o altro strumento dovrebbe riguardare:

- l'esistenza di un diritto, per gli interessati i cui dati sono trasferiti a norma del codice, di far valere le norme di quest'ultimo in quanto terzi beneficiari;
- la questione della responsabilità in caso di infrazioni alle norme del codice da parte di aderenti stabiliti al di fuori del SEE. Il codice deve includere una clausola attributiva di competenza ai sensi della quale gli interessati avranno la possibilità, in caso di violazione delle norme del codice da parte di un aderente stabilito al di fuori del SEE, di presentare un reclamo contro tale soggetto dinanzi a un'autorità di controllo del SEE e a un'autorità giurisdizionale del SEE del luogo di residenza abituale dell'interessato, in forza dei diritti di terzi beneficiari loro riconosciuti, anche a fini risarcitori. Il soggetto aderente al codice che sia stabilito al di fuori del SEE deve accettare la deci-

sione dell'interessato. Gli interessati avranno anche la possibilità di presentare reclami contro l'esportatore derivanti dal mancato rispetto del codice di condotta da parte dell'importatore dinanzi all'autorità di controllo o a un'autorità giurisdizionale del luogo di stabilimento dell'esportatore di dati o di residenza abituale dell'interessato. Tali disposizioni in materia di responsabilità dovrebbero lasciare impregiudicati i meccanismi da attuare a norma del codice, per cui anche l'organismo di monitoraggio deve poter prendere provvedimenti contro i titolari/responsabili del trattamento conformemente al codice, imponendo misure correttive. L'importatore e l'esportatore di dati devono inoltre accettare che l'interessato possa essere rappresentato da un organismo, un'organizzazione o un'associazione senza scopo di lucro alle condizioni stabilite nell'articolo 80, paragrafo 1, del GDPR;

- l'esistenza di un diritto per l'esportatore di far valere le regole del codice in quanto terzo beneficiario nei confronti di un aderente che operi in qualità di importatore;
- l'esistenza di un obbligo dell'importatore di notificare all'esportatore e all'autorità di controllo di quest'ultimo qualsiasi violazione rilevata del codice da parte dell'importatore stesso in quanto aderente al codice stabilito al di fuori del SEE e qualsiasi misura correttiva adottata dall'organismo di monitoraggio in risposta a tale violazione.

6.2 LISTA DI CONTROLLO DEGLI ELEMENTI DA INCLUDERE IN UN CODICE DI CONDOTTA DESTINATO AI TRASFERIMENTI

36. Alla luce delle garanzie fornite a norma dell'articolo 46 del GDPR dagli strumenti per i trasferimenti esistenti (come ad esempio le norme vincolanti d'impresa), e al fine di assicurare coerenza nel livello di protezione, nonché tenuto conto della sentenza Schrems II della Corte di giustizia dell'Unione europea[10], l'EDPB ritiene che gli elementi seguenti debbano figurare in un codice di condotta destinato ai trasferimenti affinché si possa considerare che tale codice fornisce garanzie adeguate:

- una descrizione dei trasferimenti previsti dal codice (natura dei dati trasferiti, categorie di interessati, paesi);
- una descrizione dei principi di protezione dei dati da rispettare a norma del codice (trasparenza, correttezza e liceità, limitazione della finalità, minimizzazione ed esattezza dei dati, limitazione del periodo di conservazione dei dati, trattamento dei dati sensibili, sicurezza, per i responsabili del trattamento conformità alle istruzioni del titolare del trattamento), comprese disposizioni sul ricorso a responsabili del trattamento o sub-responsabili del trattamento e sui trasferimenti successivi;
- le misure relative al principio di responsabilizzazione da adottare a norma del codice;
- l'istituzione di una governance adeguata tramite i responsabili della protezione dei dati o altre figure addette alla privacy che siano responsabili della conformità agli obblighi di protezione dei dati derivanti dal codice;

- l'esistenza di un programma di formazione adeguato sugli obblighi derivanti dal codice;
- l'esistenza di un meccanismo di verifica della protezione dei dati (attraverso auditor interni o esterni) o di un altro meccanismo interno finalizzato a monitorare la conformità al codice, indipendentemente dalla supervisione che deve essere effettuata dall'organismo di monitoraggio come per qualsiasi codice di condotta; mentre il meccanismo di verifica della protezione dei dati mira ad assicurare e dimostrare la conformità al codice, le verifiche eseguite dall'organismo di monitoraggio mirano a valutare se un candidato all'adesione sia idoneo, se continui a esserlo una volta che abbia aderito al codice, e se siano necessarie sanzioni in caso di violazioni;
- misure di trasparenza, tra cui la facilità di accesso, relativamente all'utilizzo del codice con particolare riguardo ai diritti dei terzi beneficiari;
- il riconoscimento agli interessati dei diritti di accesso, rettifica, cancellazione, limitazione, notifica in caso di rettifica, cancellazione o limitazione, opposizione al trattamento, nonché del diritto a non essere soggetti a decisioni basate esclusivamente sul trattamento automatizzato, compresa la profilazione, come previsti dagli articoli 12, 13, 14, 15, 16, 17, 18, 19, 21 e 22 del GDPR;
- la creazione di diritti di terzi beneficiari affinché gli interessati possano azionare le norme del codice in qualità di terzi beneficiari (nonché proporre un reclamo dinanzi all'autorità competente e agli organi giurisdizionali del SEE);
- l'esistenza, presso l'organismo di monitoraggio, di un'adeguata procedura di gestione dei reclami concernenti violazioni delle norme di protezione dei dati, che potrà essere integrata, ove opportuno, da analoghe procedure previste presso i singoli aderenti al codice;
- la garanzia che, all'atto dell'adesione al codice, il titolare/responsabile del trattamento non ha motivo di ritenere che le leggi applicabili al trattamento dei dati personali nel paese terzo di trasferimento gli impediscano di rispettare gli obblighi che gli incombono a norma del codice e di adottare, se del caso insieme all'esportatore, misure supplementari[11] al fine di garantire il livello di protezione richiesto a norma della legislazione del SEE[12]. Inoltre una descrizione delle misure da adottare (comprese la notifica all'esportatore nel SEE e l'attuazione di adeguate misure supplementari) nel caso in cui, dopo aver aderito al codice, il titolare/responsabile del trattamento del paese terzo venga a conoscenza di legislazione in tale paese terzo che impedisce all'aderente al codice di assicurare la conformità agli impegni assunti nell'ambito del codice, nonché una descrizione delle misure da adottare in caso di richieste di accesso da parte di autorità governative del paese terzo;
- i meccanismi per la gestione delle modifiche al codice;
- le conseguenze del ritiro di un aderente dal codice;
- l'impegno da parte dell'aderente al codice e dell'organismo di monitoraggio a cooperare con l'autorità di controllo del SEE;
- l'impegno da parte dell'aderente al codice ad accettare la competenza dell'autorità di controllo del SEE e delle autorità giurisdizionali del SEE in qualsiasi procedura volta a garantire il rispetto del codice di condotta;

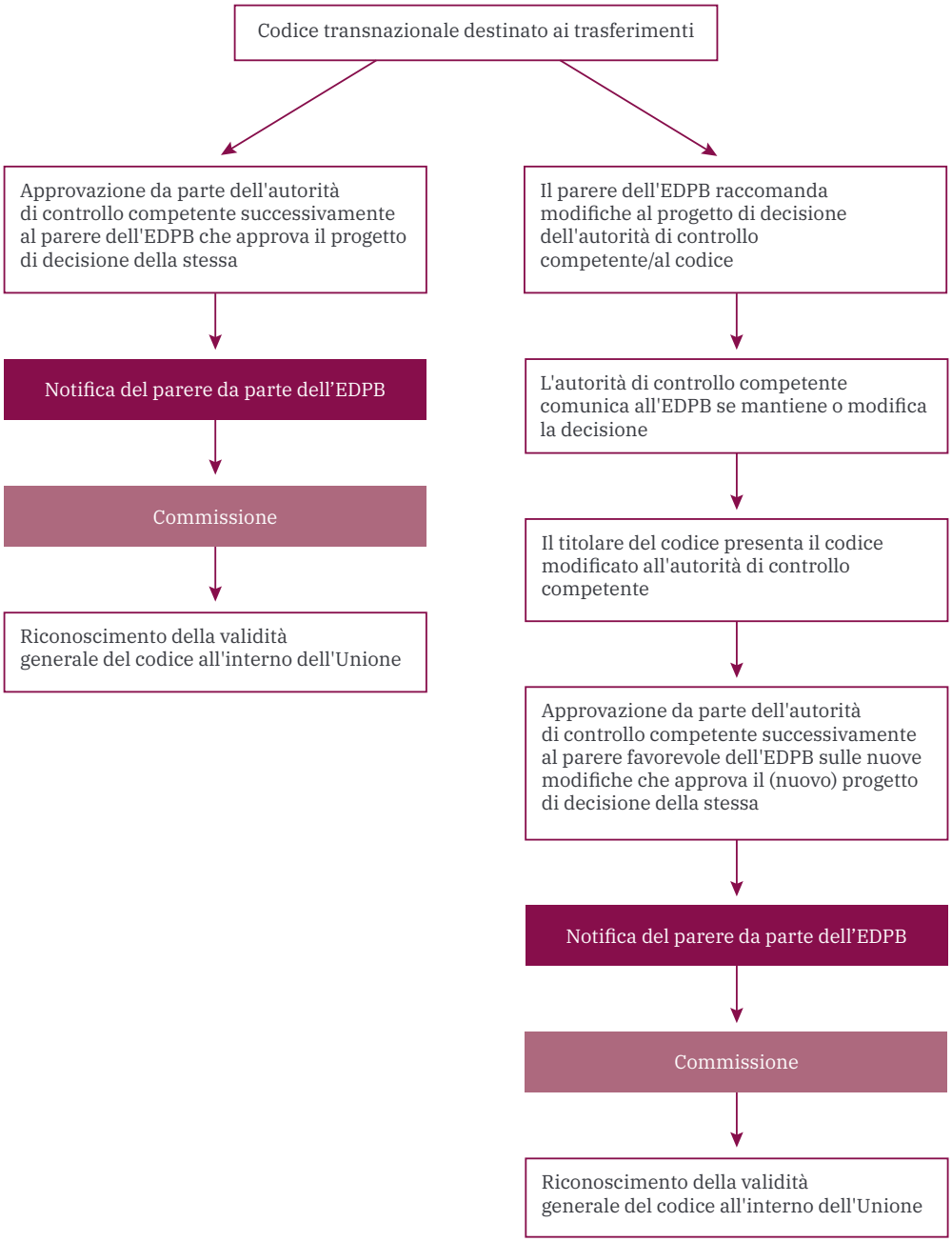
- i criteri di selezione dell'organismo di monitoraggio con riguardo al codice destinato ai trasferimenti, atti a dimostrare che l'organismo di monitoraggio dispone delle competenze richieste per svolgere il suo ruolo in modo efficace rispetto a un codice di condotta del genere.

37. In ogni caso, occorre rilevare che tali elementi costituiscono garanzie minime che potrebbero dover essere integrate con impegni e misure aggiuntivi a seconda del trasferimento in questione nell'ambito del codice di condotta.

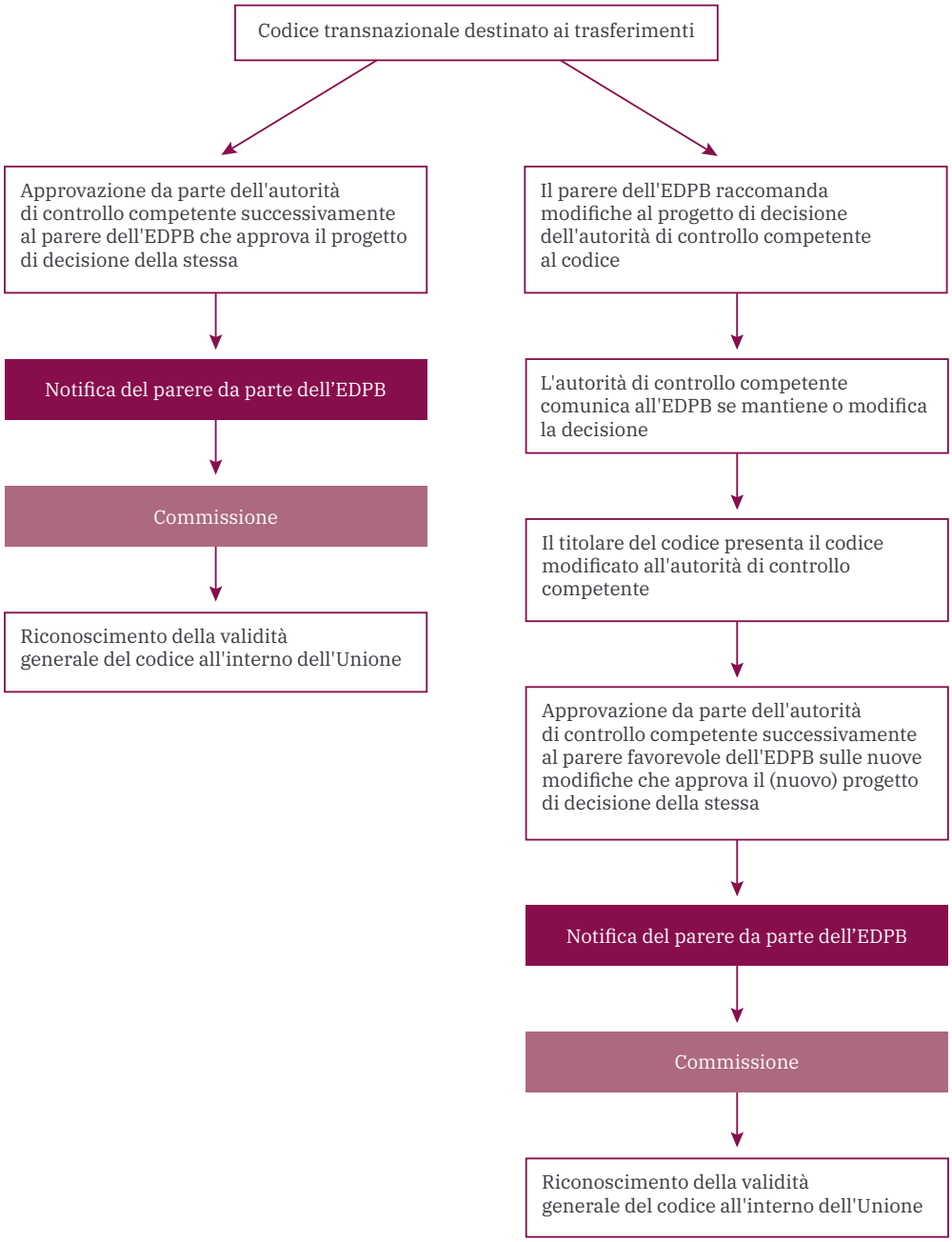
38. L'EDPB valuterà il funzionamento delle presenti linee guida alla luce dell'esperienza acquisita con la loro applicazione pratica e fornirà ulteriori indicazioni per chiarire l'applicazione degli elementi sopra elencati.

ALLEGATO 1 - ADOZIONE DI UN CODICE DI CONDOTTA PER I TRASFERIMENTI - DIAGRAMMA DI FLUSSO

A - ADOZIONE DI UN CODICE TRANSNAZIONALE DESTINATO AI TRASFERIMENTI



B - MODIFICHE A UN CODICE TRANSNAZIONALE DA UTILIZZARE COME CODICE DESTINATO AI TRASFERIMENTI



NOTE

[1] Sentenza della Corte (Grande Sezione) del 16 luglio 2020; Data Protection Commissioner / Facebook Ireland Limited, Maximillian Schrems.

[2] Nel presente documento con il termine "Stati membri" si intendono gli "Stati membri del SEE".

[3] L'esempio non pregiudica le raccomandazioni dell'EDPB 1/2020 relative alle misure che integrano gli strumenti di trasferimento.

[4] "Codice transnazionale": un codice che regola le attività di trattamento in più Stati membri. Cfr. le linee guida 1/2019, appendice 1 - Distinzione tra codici nazionali e transnazionali.

[5] Cfr. linee guida 1/2019, sezione 6.

[6] Per ulteriori dettagli sui requisiti relativi al titolare del codice, si faccia riferimento alla definizione di titolare del codice nella sezione 2 e nella sezione 5.3 delle linee guida 1/2019.

[7] Per ulteriori dettagli sulla necessità di istituire un organismo di monitoraggio nell'ambito di un codice di condotta si rimanda alle sezioni 11 e 12 delle linee guida 1/2019.

[8] Cfr. il documento dell'EDPB sulla procedura per lo sviluppo di "sessioni informali sui codici di condotta" https://edpb.europa.eu/sites/default/files/files/file1/edpb_documentproceduredesconductsessions_it.pdf.

[9] Cfr. le linee guida 1/2019, appendice 1 - Distinzione tra codici nazionali e transnazionali.

[10] Sentenza della Corte (Grande Sezione) del 16 luglio 2020; Data Protection Commissioner / Facebook Ireland Limited, Maximillian Schrems.

[11] Il Comitato europeo per la protezione dei dati ha pubblicato una raccomandazione sulle misure che integrano gli strumenti per i trasferimenti al fine di garantire la conformità al livello di protezione dei dati personali dell'UE, che può risultare utile nella valutazione relativa al paese terzo e per individuare le misure supplementari adeguate.

[12] Sul presupposto che la legislazione e le prassi che rispettano l'essenza dei diritti e delle libertà fondamentali e non vanno oltre quanto necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi di cui all'articolo 23, paragrafo 1, del regolamento (UE) 2016/679 non siano in conflitto con le garanzie specificate nel codice di condotta destinato ai trasferimenti.

Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE Versione 2.0

Adottate il 18 giugno 2021

Cronologia delle versioni

Versione 2.0	18 giugno 2021	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	10 novembre 2020	Adozione delle linee guida per la consultazione pubblica

SINTESI

Il regolamento generale sulla protezione dei dati (RGPD) dell'UE è stato adottato per un duplice scopo: agevolare la libera circolazione dei dati personali all'interno dell'Unione europea preservando al contempo i diritti e le libertà fondamentali delle persone, in particolare il loro diritto alla protezione dei dati personali.

Nella recente sentenza C-311/18 (Schrems II) la Corte di giustizia dell'Unione europea (CGUE) ricorda che la protezione concessa ai dati personali nello Spazio economico europeo (SEE) deve transitare con i dati ovunque essi siano trasferiti. Il trasferimento di dati personali verso paesi terzi non può essere un mezzo per minare o indebolire la protezione che viene garantita nel SEE. La Corte afferma ciò chiarendo inoltre che il livello di protezione nei paesi terzi non deve necessariamente essere identico a quello garantito all'interno del SEE, ma sostanzialmente equivalente. La Corte sostiene inoltre la validità delle clausole contrattuali tipo, in quanto strumento di trasferimento che può servire a garantire sul piano contrattuale un livello di protezione sostanzialmente equivalente per i dati trasferiti verso paesi terzi.

Le clausole contrattuali tipo e gli altri strumenti di trasferimento di cui all'articolo 46 del RGPD non operano in modo isolato. La Corte afferma che i titolari o responsabili del trattamento, in qualità di esportatori, hanno la responsabilità di verificare, caso per caso e, ove necessario, in collaborazione con l'importatore nel paese terzo, se il diritto o la prassi di quest'ultimo incide sull'efficacia delle garanzie adeguate contenute negli strumenti di trasferimento di cui all'articolo 46 del RGPD. In tali casi la Corte lascia comunque aperta la possibilità per gli esportatori di attuare misure supplementari che colmino queste lacune nella protezione e la portino al livello richiesto dal diritto dell'UE. La Corte non specifica di quali misure potrebbe trattarsi, ma sottolinea che gli esportatori dovranno identificarle caso per caso. Ciò è in linea con il principio di responsabilizzazione di cui all'articolo 5, paragrafo 2, del RGPD, che prevede che i titolari del trattamento siano responsabili del rispetto dei principi del suddetto regolamento relativi al trattamento dei dati personali e siano in grado di dimostrarlo.

Per aiutare gli esportatori (siano essi titolari del trattamento o responsabili del trattamento, enti privati o organismi pubblici, che trattano dati personali nell'ambito di applicazione del RGPD) nel complesso compito di valutare i paesi terzi e di individuare, se necessario, misure supplementari adeguate, il comitato europeo per la protezione dei dati (EDPB) ha adottato le presenti raccomandazioni, le quali forniscono agli esportatori una serie di passi da seguire, potenziali fonti di informazione e alcuni esempi di misure supplementari che potrebbero essere messe in atto.

Come **primo passo**, l'EDPB consiglia a voi, esportatori, di **conoscere i vostri trasferimenti**. La mappatura di tutti i trasferimenti di dati personali verso paesi terzi può essere un esercizio difficile. Essere consapevoli della destinazione dei dati personali è tuttavia necessario per garantire un livello di protezione sostanzialmente equivalente in tutti i luoghi in cui vengono trattati. Dovete inoltre veri-

ficare che i dati trasferiti siano adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali vengono trattati.
Un **secondo passo** consiste nel **verificare lo strumento di trasferimento su cui si basa il vostro trasferimento** tra quelli elencati al capo V del RGPD. Qualora la Commissione europea abbia già dichiarato il paese, la regione o il settore verso cui trasferirete i dati come adeguato, attraverso una decisione di adeguatezza ai sensi dell'articolo 45 del RGPD o della precedente direttiva 95/46 fintanto che la decisione è ancora in vigore, non dovrete adottare ulteriori misure, se non controllare che la decisione di adeguatezza sia ancora valida. In assenza di una decisione di adeguatezza, dovete fare affidamento su uno degli strumenti di trasferimento elencati all'articolo 46 del RGPD. Solo in alcuni casi sarà possibile basarsi su una delle deroghe previste dall'articolo 49 del RGPD, se le condizioni sono soddisfatte. Le deroghe non possono diventare «la norma» nella pratica, ma devono essere limitate a situazioni specifiche.

Un **terzo passo** consiste nel **valutare** se vi sia qualcosa nella legislazione e/o nelle prassi vigenti del paese terzo che possa incidere sull'efficacia delle garanzie adeguate offerte dagli strumenti di trasferimento su cui fate affidamento, nel contesto del vostro specifico trasferimento. La vostra valutazione deve concentrarsi innanzitutto sulla legislazione del paese terzo rilevante per il trasferimento e sullo strumento di trasferimento ai sensi dell'articolo 46 del RGPD su cui fate affidamento. Inoltre, l'esame delle prassi delle autorità pubbliche di paesi terzi vi permetterà di verificare se le garanzie contenute nello strumento di trasferimento possano assicurare, nella pratica, la protezione efficace dei dati personali trasferiti. L'esame di queste prassi sarà particolarmente pertinente per la valutazione nel caso in cui:

(i.) sia evidente che la legislazione del paese terzo, formalmente conforme agli standard dell'UE, non è applicata/rispettata nella pratica;

(ii.) esistano prassi incompatibili con gli impegni previsti dallo strumento di trasferimento qualora la legislazione pertinente del paese terzo sia carente;

(iii.) i dati trasferiti e/o l'importatore rientrino o possano rientrare nell'ambito di applicazione di una legislazione problematica (cioè una legislazione che pregiudica la garanzia contrattuale, prevista dallo strumento di trasferimento, di un livello di protezione sostanzialmente equivalente e non osserva le norme dell'UE in materia di diritti fondamentali, necessità e proporzionalità).

Nelle prime due situazioni, dovrete sospendere il trasferimento oppure mettere in atto misure supplementari adeguate se desiderate procedere con il trasferimento.

Nella terza situazione, considerando le incertezze relative alla potenziale applicazione al vostro trasferimento di una legislazione problematica, potete decidere di: sospendere il trasferimento; mettere in atto misure supplementari per procedere con il trasferimento; o, in alternativa, se ritenete e siete in grado di dimostrare e documentare di non avere motivo di credere che la legislazione problematica in questione verrà interpretata e/o attuata nella pratica in modo

da riguardare i vostri dati trasferiti e l'importatore, potete scegliere di procedere con il trasferimento senza mettere in atto misure supplementari.

Per definire gli elementi da prendere in considerazione nella valutazione della legislazione di un paese terzo che disciplina l'accesso ai dati da parte delle autorità pubbliche ai fini della sorveglianza, è opportuno fare riferimento alle raccomandazioni dell'EDPB relative alle garanzie essenziali europee.

Questa valutazione va condotta con la dovuta diligenza e documentata accuratamente. Le vostre autorità di controllo e/o giudiziarie competenti potrebbero richiederla e ritenervi responsabili di qualsiasi decisione da voi presa su tale base.

Un **quarto passo** consiste nell'**individuare e adottare le misure supplementari** necessarie per portare il livello di protezione dei dati trasferiti a un livello sostanzialmente equivalente a quello dell'UE. Questa misura è necessaria solo se la vostra valutazione rivela che la legislazione e/o le prassi del paese terzo incidono sull'efficacia dello strumento di trasferimento ai sensi dell'articolo 46 del RGPD su cui fate affidamento o su cui intendete fare affidamento nel contesto del vostro trasferimento. Le presenti raccomandazioni contengono (nell'allegato 2) un elenco non esaustivo di esempi di misure supplementari con alcune delle condizioni eventualmente richieste per essere efficaci. Come nel caso delle garanzie adeguate contenute negli strumenti di trasferimento di cui all'articolo 46, alcune misure supplementari possono essere efficaci in alcuni paesi, ma non necessariamente in altri. Sarete responsabili della valutazione della loro efficacia nel contesto del trasferimento e alla luce della legislazione e delle prassi del paese terzo e dello strumento di trasferimento su cui fate affidamento, in quanto sarete ritenuti responsabili di qualsiasi decisione presa su tale base. Ciò potrebbe anche richiedere la combinazione di più misure supplementari. In ultima analisi, potreste concludere che nessuna misura supplementare è in grado di garantire un livello di protezione sostanzialmente equivalente per il vostro specifico trasferimento. Ove nessuna misura supplementare sia adeguata, dovete evitare, sospendere o interrompere il trasferimento per evitare di pregiudicare il livello di protezione dei dati personali. Anche questa valutazione delle misure supplementari va condotta con la dovuta diligenza e documentata.

Un **quinto passo** consiste nell'**adozione** di eventuali **passi procedurali formali** richiesti dall'adozione della vostra misura supplementare, a seconda dello strumento di trasferimento di cui all'articolo 46 del RGPD su cui fate affidamento. Le presenti raccomandazioni riportano nel dettaglio alcune di queste formalità; in alcuni casi potrebbe essere necessario consultare le autorità di controllo competenti.

Il **sesto e ultimo passo** consiste nel **riesaminare** a intervalli adeguati il livello di protezione dei dati personali che trasferite verso paesi terzi e di controllare se vi siano stati o vi saranno sviluppi che possano influire in questo senso. Il principio di responsabilizzazione richiede vigilanza continua rispetto al livello di protezione dei dati personali.

Le autorità di controllo continueranno a esercitare il mandato loro conferito di monitorare l'applicazione del RGPD e farlo rispettare. Le autorità di controllo terranno in debita considerazione le azioni intraprese dagli esportatori per garantire che i dati da essi trasferiti godano di un livello di protezione sostanzialmente equivalente. Come ricorda la Corte, le autorità di controllo sospenderanno o vieteranno il trasferimento dei dati nei casi in cui ritengano che non possa essere garantito un livello di protezione sostanzialmente equivalente, a seguito di un'indagine o di un reclamo.

Le autorità di controllo continueranno a sviluppare orientamenti per gli esportatori e a coordinare le attività in seno all'EDPB per garantire la coerenza nell'applicazione della legislazione dell'UE in materia di protezione dei dati.

Indice

1 Responsabilizzazione nel trasferimento dei dati

2 Cronoprogramma per applicare il principio di responsabilizzazione al trasferimento dei dati nella pratica
- 2.1 Primo passo: conoscere i propri trasferimenti
- 2.2 Secondo passo: individuare gli strumenti di trasferimento su cui fate affidamento
- 2.3 Terzo passo: valutare se lo strumento di trasferimento di cui all'articolo 46 del RGPD su cui si fa affidamento è efficace alla luce di tutte le circostanze del trasferimento
- 2.4 Quarto passo: adozione di misure supplementari
- 2.5 Quinto passo: passaggi procedurali se avete individuato misure supplementari efficaci
- 2.6 Sesto passo: rivalutare a intervalli appropriati

3 Conclusioni

ALLEGATO 1: DEFINIZIONI

ALLEGATO 2: ESEMPI DI MISURE SUPPLEMENTARI
- 2.1 Misure tecniche
- 2.2 Misure contrattuali supplementari
- 2.3 Misure organizzative

ALLEGATO 3: POSSIBILI FONTI DI INFORMAZIONI PER VALUTARE UN PAESE TERZO

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettera e), del regolamento 2016/679/UE del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in appresso: il «RGPD»),

visto l'accordo sullo Spazio economico europeo (SEE), in particolare l'allegato XI e il protocollo 37 dello stesso, modificato dalla decisione del comitato misto SEE n. 154/2018, del 6 luglio 2018[1],

visto l'articolo 12 e l'articolo 22 del regolamento interno,

considerando quanto segue:

(1) Nella sentenza del 16 luglio 2020 *Data Protection Commissioner* contro *Facebook Ireland Limited e Maximillian Schrems*, C-311/18, la Corte di giustizia dell'Unione europea (CGUE) conclude che l'articolo 46, paragrafo 1, e l'articolo 46, paragrafo 2, lettera c), del RGPD, devono essere interpretati nel senso che le garanzie adeguate, i diritti azionabili e i mezzi di ricorso effettivi richiesti da tali disposizioni devono garantire che i diritti delle persone i cui dati personali sono trasferiti verso un paese terzo sul fondamento di clausole tipo di protezione dei dati godano di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta dei diritti fondamentali dell'Unione europea[2].

(2) Come sottolineato dalla Corte, un livello di protezione delle persone fisiche sostanzialmente equivalente a quello garantito all'interno dell'Unione dal RGPD, letto alla luce della Carta, deve essere garantito indipendentemente dalla disposizione del capo V sul cui fondamento viene effettuato un trasferimento di dati personali verso un paese terzo. Le disposizioni del capo V mirano a garantire la continuità del livello elevato di tale protezione in caso di trasferimento di dati personali verso un paese terzo[3].

(3) Il considerando 108 e l'articolo 46, paragrafo 1, del RGPD, prevedono che, in mancanza di una decisione di adeguatezza dell'Unione, il titolare del trattamento o il responsabile del trattamento dovrebbe provvedere a compensare la carenza di protezione dei dati in un paese terzo con adeguate garanzie a tutela dell'interessato. Il titolare del trattamento o il responsabile del trattamento può fornire garanzie adeguate, senza richiedere un'autorizzazione specifica da parte di un'autorità di controllo, utilizzando uno degli strumenti di trasferimento elencati all'articolo 46, paragrafo 2, del RGPD, come le clausole tipo di protezione dei dati.

(4) La Corte chiarisce che le clausole tipo di protezione dei dati adottate dalla Commissione hanno il solo scopo di fornire garanzie contrattuali che si ap-

plicano in modo uniforme in tutti i paesi terzi ai titolari del trattamento e ai responsabili del trattamento stabiliti nell'Unione. Visto il loro carattere contrattuale, le clausole tipo di protezione dei dati non possono vincolare le autorità pubbliche di paesi terzi, poiché queste ultime non sono parti del contratto. Di conseguenza, gli esportatori di dati potrebbero dover integrare le garanzie contenute in tali clausole tipo di protezione dei dati con misure supplementari per garantire il rispetto del livello di protezione richiesto dal diritto dell'Unione in un determinato paese terzo. La Corte fa riferimento al considerando 109 del RGPD, che menziona questa possibilità e incoraggia i titolari del trattamento e i responsabili del trattamento ad avvalersene[4].

(5) La Corte ha affermato che incombe anzitutto all'esportatore dei dati verificare, caso per caso e, eventualmente, in collaborazione con l'importatore dei dati, se il diritto del paese terzo di destinazione garantisce un livello di protezione sostanzialmente equivalente, alla luce del diritto dell'Unione, dei dati personali trasferiti sulla base di clausole tipo di protezione dei dati, fornendo, se necessario, garanzie supplementari rispetto a quelle offerte da tali clausole[5].

(6) Qualora il titolare del trattamento o il responsabile del trattamento, stabiliti nell'Unione, non possano adottare misure supplementari sufficienti a garantire un livello di protezione sostanzialmente equivalente ai sensi del diritto dell'Unione, essi o, in subordine, l'autorità di controllo competente, sono tenuti a sospendere o mettere fine al trasferimento di dati personali verso il paese terzo interessato[6].

(7) Il RGPD o la Corte non definiscono né specificano le «garanzie supplementari» o le «misure supplementari» alle garanzie degli strumenti di trasferimento elencati all'articolo 46, paragrafo 2, del RGPD, che i titolari del trattamento e i responsabili del trattamento possono adottare per garantire il rispetto del livello di protezione richiesto dal diritto dell'Unione in un determinato paese terzo.

(8) L'EDPB ha deciso, di propria iniziativa, di esaminare la questione e di fornire ai titolari e ai responsabili del trattamento, in qualità di esportatori, raccomandazioni sul processo che possono seguire per individuare e adottare misure supplementari. Tali raccomandazioni mirano a fornire agli esportatori una metodologia per determinare se e quali misure supplementari dovrebbero essere adottate per i loro trasferimenti. È responsabilità primaria degli esportatori garantire che nel paese terzo sia offerto ai dati trasferiti un livello di protezione sostanzialmente equivalente a quello garantito nel SEE. Con queste raccomandazioni, l'EDPB mira a incoraggiare l'applicazione coerente del RGPD e della sentenza della Corte, conformemente al proprio mandato[7].

HA ADOTTATO LA SEGUENTE RACCOMANDAZIONE:

1. RESPONSABILIZZAZIONE NEL TRASFERIMENTO DEI DATI

1. Il diritto primario dell'Unione considera il diritto alla protezione dei dati come un diritto fondamentale[8]. Di conseguenza, il diritto alla protezione dei dati gode di un elevato livello di protezione e possono essere apportate limitazioni solo se sono previste dalla legge, rispettano il contenuto essenziale di detto diritto, rispettano il principio di proporzionalità, sono necessarie e rispondono effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui[9]. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità[10].
2. Un livello di protezione sostanzialmente equivalente a quello garantito nell'UE deve accompagnare i dati quando sono trasferiti verso paesi terzi al di fuori del SEE, per garantire che il livello di protezione assicurato dal RGPD non sia pregiudicato, sia durante sia dopo il trasferimento.
3. Il diritto alla protezione dei dati ha un carattere attivo, ossia impone agli esportatori e agli importatori (siano essi titolari del trattamento e/o responsabili del trattamento) di andare oltre il riconoscimento o il rispetto passivo di tale diritto[11]. I titolari e i responsabili del trattamento devono cercare di rispettare il diritto alla protezione dei dati in modo attivo e continuo, attuando misure giuridiche, tecniche e organizzative che ne garantiscano l'efficacia. Essi devono inoltre essere in grado di comprovare questi sforzi agli interessati e alle autorità di controllo in materia di protezione dei dati. Questo è il cosiddetto principio di responsabilizzazione[12].
4. Il principio di responsabilizzazione, necessario per garantire l'effettiva applicazione del livello di protezione conferito dal RGPD, si applica anche ai trasferimenti di dati verso paesi terzi[13], in quanto si tratta di una forma di trattamento dei dati in sé[14]. Come sottolineato dalla Corte nella sentenza, un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione dal RGPD, letto alla luce della Carta, deve essere garantito indipendentemente da quale sia la disposizione di detto capo sul cui fondamento viene effettuato un trasferimento di dati personali verso un paese terzo[15].
5. Nella sentenza Schrems II, la Corte sottolinea la responsabilità degli esportatori e degli importatori di garantire che il trattamento dei dati personali sia e continui a essere effettuato nel rispetto del livello di protezione stabilito dal diritto dell'Unione in materia di protezione dei dati e di sospendere il trasferimento e/o risolvere il contratto qualora l'importatore dei dati non sia o non sia più in grado di rispettare le clausole tipo di protezione dei dati inserite nel relativo contratto tra l'esportatore e l'importatore[16]. Il titolare del trattamento o il responsabile del trattamento che agisce in qualità di esportatore deve garantire che gli importatori collaborino con l'esportatore, se del caso, nell'adempimento di tali responsabilità, tenendolo informato, ad esempio, di qualsiasi sviluppo che influisca sul livello di protezione dei dati personali ricevuti nel paese dell'importatore[17]. Tali responsabilità sono un'applicazione del principio di responsabilizzazione in materia di trasferimenti di dati ai sensi del RGPD[18].

2. CRONOPROGRAMMA PER APPLICARE IL PRINCIPIO DI RESPONSABILIZZAZIONE AL TRASFERIMENTO DEI DATI NELLA PRATICA

6. Quello che segue è un cronoprogramma dei passi da compiere per scoprire se voi (esportatori di dati) dovete mettere in atto misure supplementari per poter trasferire legalmente i dati al di fuori del SEE. Nel presente documento, per «voi» si intendono i titolari del trattamento o i responsabili del trattamento che agiscono in qualità di esportatori di dati[19] e trattano dati personali nell'ambito di applicazione del RGPD (compreso il trattamento da parte di enti privati e organismi pubblici in caso di trasferimento di dati a enti privati)[20]. Per quanto riguarda i trasferimenti di dati personali effettuati tra organismi pubblici, *le linee guida 2/2020 sull'articolo 46, paragrafo 2, lettera a), e sull'articolo 46, paragrafo 3, lettera b), del regolamento 2016/679 per i trasferimenti di dati personali tra autorità e organismi pubblici del SEE ed extra SEE* forniscono orientamenti specifici[21].
7. Dovrete documentare adeguatamente questa valutazione e le misure supplementari da voi selezionate e attuate e, su richiesta, mettere a disposizione dell'autorità di controllo competente tale documentazione[22].

2.1 PRIMO PASSO: CONOSCERE I PROPRI TRASFERIMENTI

8. Per sapere cosa può essere necessario affinché voi (l'esportatore di dati) possiate continuare a effettuare trasferimenti di dati personali o possiate effettuarne di nuovi[23], il primo passo consiste nell'assicurarvi di essere pienamente consapevoli dei vostri trasferimenti (conoscere i vostri trasferimenti). La registrazione e la mappatura di tutti i trasferimenti può essere un esercizio complesso per quei soggetti che sono coinvolti in trasferimenti multipli, diversificati e regolari con paesi terzi e che ricorrono a una serie di responsabili del trattamento a vari livelli. Conoscere i propri trasferimenti è un primo passo essenziale per adempiere ai propri obblighi ai sensi del principio di responsabilizzazione.
9. Per acquisire piena consapevolezza dei vostri trasferimenti, potete basarvi sui registri delle attività di trattamento che potreste essere obbligati a tenere in qualità di titolari del trattamento o di responsabili del trattamento ai sensi dell'articolo 30 del RGPD[24]. Possono esservi di aiuto anche le attività già messe in atto al fine di adempiere agli obblighi di informazione degli interessati ai sensi dell'articolo 13, paragrafo 1, lettera f), e dell'articolo 14, paragrafo 1, lettera f), del RGPD, relativamente ai trasferimenti dei loro dati personali da voi effettuati verso paesi terzi[25].
10. Nel mappare i trasferimenti, non dimenticate di tenere conto anche dei trasferimenti successivi, ad esempio se i vostri responsabili del trattamento al di fuori del SEE trasferiscono i dati personali che avete affidato loro a un responsabile del trattamento di secondo livello in un altro paese terzo o nello stesso paese terzo[26].
11. In linea con il principio della «minimizzazione dei dati»[27] del RGPD, dovete

verificare che i dati trasferiti siano adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali vengono trattati.

12. Queste attività devono essere svolte prima di qualsiasi trasferimento e aggiornate prima di riprendere i trasferimenti dopo la sospensione delle operazioni di trasferimento dei dati: dovete sapere dove si trovano o possono essere trattati dagli importatori i dati personali che avete esportato (mappa delle destinazioni).
13. Occorre tenere presente che anche l'accesso remoto da un paese terzo (ad esempio in situazioni di supporto) e/o l'archiviazione in una piattaforma cloud situata al di fuori del SEE offerta da un fornitore di servizi sono considerati un trasferimento[28]. In particolare, se si utilizza un'infrastruttura cloud internazionale, dovete valutare se i dati saranno trasferiti in paesi terzi e dove, a meno che il fornitore del cloud sia stabilito nel SEE e dichiari espressamente nel contratto che i dati non saranno in alcun modo elaborati in paesi terzi.

2.2 SECONDO PASSO: INDIVIDUARE GLI STRUMENTI DI TRASFERIMENTO SU CUI FATE AFFIDAMENTO

14. Un secondo passo da compiere consiste nell'individuare gli strumenti di trasferimento su cui fare affidamento tra quelli elencati e previsti nel capo V del RGPD.

Decisioni di adeguatezza

15. La Commissione europea può riconoscere, attraverso **decisioni di adeguatezza** relative ad alcuni o a tutti i paesi terzi verso i quali trasferite i dati personali, che essi offrono un adeguato livello di protezione dei dati personali[29].
16. L'effetto di una tale decisione di adeguatezza è che i dati personali possono circolare dal SEE verso quel paese terzo senza che sia necessario uno strumento di trasferimento ai sensi dell'articolo 46 del RGPD.
17. Le decisioni di adeguatezza possono riguardare un paese nel suo insieme o essere limitate a una parte di esso. Esse possono inoltre riguardare tutti i trasferimenti di dati verso un paese o essere limitate ad alcuni tipi di trasferimenti (ad esempio in un settore)[30].
18. La Commissione europea pubblica l'elenco delle decisioni di adeguatezza sul suo sito web[31].
19. Se trasferite dati personali verso paesi terzi, regioni o settori cui si riferisce una decisione di adeguatezza della Commissione (nella misura in cui sia applicabile), **non dovete adottare ulteriori misure come descritto nelle presenti raccomandazioni**[32]. Tuttavia, dovete comunque controllare se le decisioni di adeguatezza pertinenti per detti trasferimenti sono revocate o invalidate[33].
20. Tuttavia, le decisioni di adeguatezza non impediscono agli interessati di

presentare un reclamo, né impediscono alle autorità di controllo di adire un giudice nazionale in caso di dubbi sulla validità di una decisione, affinché il giudice nazionale possa adire la CGUE per l'esame di tale validità[34].

Esempio:

Un cittadino dell'UE, il sig. Schrems, ha presentato una denuncia nel giugno 2013 presso la Commissione irlandese per la protezione dei dati (DPC) e ha chiesto a tale autorità di controllo di vietare o sospendere il trasferimento dei suoi dati personali da Facebook Ireland agli Stati Uniti, in quanto riteneva che la legge e la prassi degli Stati Uniti non garantissero una protezione adeguata dei dati personali detenuti nel loro territorio rispetto alle attività di controllo che vi erano svolte dalle autorità pubbliche. La DPC ha respinto la denuncia a motivo del fatto, in particolare, che nella decisione 2000/520 la Commissione europea aveva ritenuto che, nell'ambito del regime dell'approdo sicuro, gli Stati Uniti garantissero un livello adeguato di protezione dei dati personali trasferiti (decisione sull'approdo sicuro). Il sig. Schrems ha impugnato la decisione della DPC e la Corte d'appello irlandese ha sottoposto alla Corte di giustizia dell'Unione europea (CGUE) un quesito sulla validità della decisione 2000/520. La CGUE ha successivamente deciso di invalidare la decisione 2000/520 della Commissione sull'adeguatezza della protezione fornita dai principi di approdo sicuro in materia di riservatezza[35].

Articolo 46 del RGPD – Strumenti di trasferimento

21. L'articolo 46 del RGPD elenca una serie di strumenti di trasferimento contenenti «garanzie adeguate» che gli esportatori possono utilizzare per trasferire dati personali verso paesi terzi in assenza di decisioni di adeguatezza. I principali tipi di strumenti di trasferimento di cui all'articolo 46 del RGPD sono:

- le clausole contrattuali tipo di protezione dei dati;
- le norme vincolanti d'impresa;
- i codici di condotta;
- i meccanismi di certificazione;
- clausole contrattuali ad hoc.

22. Qualunque sia lo strumento di trasferimento di cui all'articolo 46 del RGPD che si sceglie di adottare, è necessario garantire che, nel complesso, i dati personali trasferiti godano di un livello di protezione sostanzialmente equivalente.

23. Gli strumenti di trasferimento di cui all'articolo 46 del RGPD contengono principalmente garanzie adeguate di natura contrattuale che possono essere applicate ai trasferimenti verso tutti i paesi terzi. La situazione nel paese terzo verso il quale sono trasferiti i dati può comunque richiedere di integrare questi strumenti di trasferimento e le garanzie in essi contenute con misure integrative («misure supplementari») volte a garantire un livello di protezione sostanzialmente equivalente[36].

Deroghe

24. Oltre alle decisioni di adeguatezza e agli strumenti di trasferimento di cui all'articolo 46 del RGPD, quest'ultimo contiene una terza via che consente il trasferimento di dati personali in determinate situazioni. A determinate condizioni specifiche, potrebbe essere comunque possibile trasferire dati personali in base a una delle deroghe elencate all'articolo 49 del RGPD.

25. Tale articolo ha carattere eccezionale e le deroghe in esso previste devono essere interpretate in modo da non contraddire la loro stessa natura, trattandosi di eccezioni alla regola secondo cui i dati personali non possono essere trasferiti verso un paese terzo, a meno che tale paese non preveda un livello adeguato di protezione dei dati o, in alternativa, non siano messe in atto garanzie adeguate. Le eccezioni non possono diventare «la regola» nella pratica, ma devono essere limitate a situazioni specifiche. L'EDPB ha emanato le linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679[37].

26. Prima di fare affidamento su una deroga di cui all'articolo 49 del RGPD dovete verificare se il trasferimento soddisfa le rigorose condizioni previste da questa disposizione per ciascuna di esse.

***

27. Se il vostro trasferimento non ha base giuridica né in una decisione di adeguatezza, né in una deroga di cui all'articolo 49, dovete continuare con il terzo passo.

2.3 TERZO PASSO: VALUTARE SE LO STRUMENTO DI TRASFERIMENTO DI CUI ALL'ARTICOLO 46 DEL RGPD SU CUI SI FA AFFIDAMENTO È EFFICACE ALLA LUCE DI TUTTE LE CIRCOSTANZE DEL TRASFERIMENTO

28. Lo strumento di trasferimento selezionato di cui all'articolo 46 del RGPD deve essere efficace nel garantire che il livello di protezione assicurato dal RGPD non sia pregiudicato dal trasferimento nella pratica[38].

29. In particolare, la protezione dei dati personali trasferiti nel paese terzo deve essere sostanzialmente equivalente a quella garantita nel SEE dal RGPD, letto alla luce della Carta dei diritti fondamentali dell'UE[39]. Ciò non avviene se l'importatore di dati non è in grado di adempiere agli obblighi previsti dallo strumento di trasferimento prescelto ai sensi dell'articolo 46 del RGPD a causa della legislazione e delle prassi del paese terzo applicabili al trasferimento, anche durante il transito dei dati dall'esportatore al paese dell'importatore[40].

30. È necessario prima di tutto valutare, se del caso in collaborazione con l'importatore, se vi siano elementi nel diritto e/o nelle prassi vigenti[41] nel paese terzo che possano incidere sull'efficacia delle garanzie adeguate offerte dallo strumento di trasferimento di cui all'articolo 46 del RGPD su cui si fa affidamento, nel contesto dello specifico trasferimento. Ciò comporta l'esigenza

di determinare se il trasferimento in questione rientri o meno nell'ambito di applicazione della legislazione e/o delle prassi che potrebbero incidere sull'efficacia dello strumento di trasferimento utilizzato di cui all'articolo 46 del RGPD. La valutazione richiesta deve basarsi innanzitutto sulla legislazione disponibile al pubblico.

31. Questa valutazione deve contenere elementi riguardanti l'accesso ai dati da parte delle autorità pubbliche del paese terzo del vostro importatore, quali ad esempio:

- elementi relativi alla possibilità o meno, per le autorità pubbliche del paese terzo del vostro importatore, di tentare di accedere ai dati, indipendentemente dal fatto che tale accesso sia effettuato con o senza la consapevolezza dell'importatore, alla luce della legislazione, della prassi e dei precedenti segnalati;
- elementi relativi alla capacità o meno, per le autorità pubbliche del paese terzo del vostro importatore, di accedere ai dati attraverso l'importatore stesso o attraverso i fornitori di telecomunicazioni o i canali di comunicazione, alla luce dei poteri giuridici e delle risorse tecniche, finanziarie e umane a loro disposizione e dei precedenti segnalati.

Individuazione di legislazione e prassi pertinenti alla luce di tutte le circostanze del trasferimento

32. Occorre esaminare le caratteristiche di ciascun trasferimento e determinare se l'ordinamento giuridico nazionale e/o le prassi vigenti del paese verso cui i dati vengono trasferiti (o successivamente trasferiti) influiscano sui vostri trasferimenti. L'ambito della vostra valutazione è pertanto limitato alla legislazione e alle prassi pertinenti per la protezione dei dati specificamente trasferiti, a differenza di quanto avviene con le valutazioni di adeguatezza generali e di ampia portata svolte dalla Commissione europea in conformità dell'articolo 45 del RGPD.

33. Il contesto giuridico e/o le prassi applicabili dipenderanno dalle circostanze specifiche del vostro trasferimento, in particolare dai seguenti elementi:

- finalità per le quali i dati vengono trasferiti ed elaborati (ad esempio marketing, risorse umane, archiviazione, supporto informatico, test clinici);
- natura dei soggetti coinvolti nel trattamento (pubblica/privata; titolare del trattamento/responsabile del trattamento);
- settore in cui avviene il trasferimento (ad esempio adtech, telecomunicazioni, finanziario, ecc.);
- categorie di dati personali trasferiti (ad esempio i dati personali che si riferiscono a minori possono rientrare nell'ambito di applicazione di una legislazione specifica del paese terzo)[42];
- conservazione dei dati nel paese terzo o accesso remoto ai dati conservati all'interno dell'UE/SEE;
- formato dei dati da trasferire (ad esempio in chiaro/pseudonimizzati o cifrati)[43];
- possibilità che i dati siano soggetti a trasferimenti successivi dal paese terzo

verso un altro paese terzo[44].

34. La valutazione deve prendere in considerazione tutti i soggetti che partecipano al trasferimento (ad esempio, titolari del trattamento, responsabili del trattamento a vari livelli che trattano i dati nel paese terzo), così come sono stati individuati nell'esercizio di mappatura dei trasferimenti. Quanto maggiore è il numero dei titolari del trattamento, dei responsabili del trattamento o degli importatori coinvolti, tanto più complessa sarà la valutazione, nella quale occorre anche tener conto di eventuali trasferimenti successivi previsti.

35. Dovreste in ogni caso prestare particolare attenzione a tutte le normative pertinenti, in particolare quelle che stabiliscono i requisiti per la comunicazione dei dati personali alle autorità pubbliche o che conferiscono a tali autorità poteri di accesso ai dati personali (ad esempio in applicazione del diritto penale, per la vigilanza prevista dalle norme o per scopi di sicurezza nazionale). Se tali requisiti o poteri limitano i diritti fondamentali degli interessati, pur rispettando la loro essenza ed essendo necessari e proporzionati in una società democratica per salvaguardare importanti obiettivi riconosciuti anche nel diritto dell'Unione e degli Stati membri dell'UE[45], non possono pregiudicare gli impegni previsti dallo strumento di trasferimento di cui all'articolo 46 del RGPD su cui si fa affidamento.

36. Dovrete valutare le norme e le prassi pertinenti di carattere generale nella misura in cui hanno un impatto sull'effettiva applicazione delle garanzie contenute nello strumento di trasferimento di cui all'articolo 46 del RGPD.

37. Nell'effettuare tale valutazione, sono pertinenti anche diversi aspetti dell'ordinamento giuridico di tale paese terzo, quali gli elementi elencati all'articolo 45, paragrafo 2, del RGPD. Ad esempio, la situazione dello stato di diritto in un paese terzo può essere pertinente per valutare l'efficacia dei meccanismi disponibili per ottenere un ricorso (in sede giudiziale) contro l'accesso illegale ai dati personali da parte del governo. L'esistenza di una legge di ampio respiro sulla protezione dei dati o di un'autorità indipendente per la protezione dei dati, nonché il rispetto degli strumenti internazionali che prevedono garanzie di protezione dei dati, possono contribuire a garantire la proporzionalità dell'ingerenza del governo.

38. Gli obblighi o i poteri derivanti da tali leggi e prassi saranno ritenuti in contrasto/incompatibili con gli impegni previsti dallo strumento di trasferimento di cui all'articolo 46 del RGPD qualora[46]:

- non rispettino l'essenza dei diritti e delle libertà fondamentali della Carta dei diritti fondamentali dell'UE; oppure
- vadano oltre quanto necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi importanti riconosciuti anche dal diritto dell'Unione e degli Stati membri, come quelli di cui all'articolo 23, paragrafo 1, del RGPD.

39. Dovreste verificare che gli impegni dell'importatore di dati che consentono agli interessati di esercitare i loro diritti, come previsti dallo strumento di trasferimento di cui all'articolo 46 del RGPD [quali le richieste di accesso, ret-

tifica e cancellazione dei dati trasferiti, nonché l'esistenza di mezzi di ricorso (in sede giudiziale)], trovino effettiva applicazione nella pratica e non siano ostacolati dal diritto e/o dalle prassi del paese terzo di destinazione.

40. Le norme dell'Unione, quali gli articoli 47 e 52 della Carta dei diritti fondamentali dell'Unione europea, devono essere utilizzate come riferimento, in particolare per valutare se tale accesso da parte delle autorità pubbliche sia limitato a quanto necessario e proporzionato in una società democratica e se agli interessati sia consentito un ricorso effettivo.

41. Le raccomandazioni dell'EDPB relative alle garanzie essenziali europee[47] chiariscono gli elementi che devono essere valutati per determinare se il quadro giuridico che disciplina l'accesso ai dati personali da parte delle autorità pubbliche in un paese terzo, siano esse agenzie di sicurezza nazionale o autorità incaricate dell'applicazione della legge, possa essere considerato un'ingerenza giustificabile[48] oppure no. In particolare, occorre considerare attentamente questo aspetto quando la legislazione che disciplina l'accesso ai dati da parte delle autorità pubbliche è ambigua o non è disponibile al pubblico. Il primo requisito delle garanzie essenziali europee è la presenza di un quadro giuridico che contempli tale accesso, ove previsto, che sia disponibile al pubblico e sufficientemente chiaro.

42. Applicate ai trasferimenti di dati basati sugli strumenti di cui all'articolo 46, le raccomandazioni dell'EDPB relative alle garanzie essenziali europee possono guidare l'esportatore di dati nel valutare se i poteri in questione interferiscono in modo ingiustificato con gli obblighi dell'esportatore e dell'importatore di garantire la sostanziale equivalenza ai sensi del RGPD o conformemente agli impegni previsti dallo strumento di trasferimento. L'insussistenza di un livello di protezione sostanzialmente equivalente sarà particolarmente evidente laddove la legislazione e/o le prassi del paese terzo interessato dal trasferimento non soddisfino i requisiti delle garanzie essenziali europee. L'EDPB ribadisce che le garanzie essenziali europee sono uno standard di riferimento per valutare l'ingerenza che le misure di sorveglianza di paesi terzi comportano nel contesto dei trasferimenti internazionali di dati. Tali standard derivano dal diritto dell'UE e dalla giurisprudenza della CGUE e della Corte CEDU, che è vincolante per gli Stati membri dell'UE.

43. La vostra valutazione deve basarsi innanzitutto sulla legislazione disponibile al pubblico. Inoltre, l'esame delle prassi delle autorità pubbliche di paesi terzi vi permetterà di verificare se le garanzie adeguate contenute nello strumento di trasferimento di cui all'articolo 46 del RGPD possano essere sufficienti a garantire, in concreto, la protezione efficace dei dati personali trasferiti[49]. L'esame delle prassi vigenti nel paese terzo sarà particolarmente importante ai fini della vostra valutazione nelle situazioni descritte di seguito.

    43.1 **La legislazione pertinente nel paese terzo potrebbe essere formalmente allineata alle norme dell'UE in materia di diritti e libertà fondamentali, nonché alla necessità e alla proporzionalità delle restrizioni ivi contemplate**. Tuttavia, le prassi delle autorità pubbliche di tale paese terzo (per esempio nell'accedere a dati personali detenuti

da soggetti privati o nell'attuare o meno la legislazione in quanto organismi di controllo o giudiziari) potrebbero chiaramente indicare che non applicano legislazione che disciplina, in linea di principio, le loro attività o non si conformano a tale legislazione. In questo caso, dovete tenere conto di tali prassi nella vostra valutazione e considerare che lo strumento di cui all'articolo 46 del RGPD non sarà in grado di garantire efficacemente, di per sé (ossia in assenza di misure supplementari), un livello di protezione sostanzialmente equivalente. In tal caso, se desiderate procedere con il trasferimento, dovrete mettere in atto misure supplementari adeguate.

43.2 **Nel paese terzo potrebbe mancare legislazione pertinente (per esempio in materia di accesso a dati personali detenuti dal settore privato)**. In questo caso non potete concludere automaticamente sulla base di tale assenza che il vostro strumento di trasferimento di cui all'articolo 46 del RGPD possa essere efficacemente applicato. Dovrete verificare l'eventuale presenza di indicazioni di prassi vigenti nel paese che sono incompatibili con il diritto dell'UE e con gli impegni previsti dallo strumento di trasferimento di cui all'articolo 46 del RGPD. Se esistono prassi incompatibili, lo strumento di trasferimento di cui all'articolo 46 del RGPD non potrà garantire efficacemente, di per sé (ossia in assenza di misure supplementari), un livello di protezione sostanzialmente equivalente. In tal caso, se desiderate procedere con il trasferimento, dovrete mettere in atto misure supplementari adeguate.

43.3 **Dalla valutazione può emergere che la legislazione pertinente nel paese terzo potrebbe essere problematica[50] e che i dati trasferiti e/o l'importatore in questione rientrano o possono rientrare nell'ambito di applicazione di tale legislazione problematica[51]**.

Considerando le incertezze relative alla potenziale applicazione al vostro trasferimento di una legislazione problematica, potete quindi decidere di:

- sospendere il trasferimento;
- mettere in atto misure supplementari[52] per prevenire il rischio che possano essere applicate, nei confronti del vostro importatore e/o dei vostri dati trasferiti, norme e/o prassi del paese terzo dell'importatore di dati che siano atte a pregiudicare le garanzie contrattuali, previste dallo strumento di trasferimento, di un livello di protezione sostanzialmente equivalente a quella garantita nel SEE; oppure
- in alternativa, potete decidere di procedere con il trasferimento senza la necessità di mettere in atto misure supplementari, se ritenete di non avere motivo di credere che la legislazione problematica pertinente verrà applicata, in concreto, nei confronti dei vostri dati trasferiti e/o dell'importatore. Dovrete avere dimostrato e documentato, mediante la vostra valutazione, ove opportuno in collaborazione con l'importatore, che la normativa non viene interpretata e/o applicata nella pratica in modo tale da riguardare i dati trasferiti e l'importatore, tenendo inoltre

conto dell'esperienza di altri soggetti che operano nello stesso settore e/o in relazione a dati personali trasferiti di natura analoga, nonché delle altre fonti di informazioni descritte qui di seguito[53].

Pertanto, sarà necessario che abbiate dimostrato e documentato con una relazione dettagliata[54] che la legislazione problematica non troverà applicazione in concreto nei confronti dei dati trasferiti e/o dell'importatore e che, di conseguenza, non impedirà all'importatore di assolvere gli obblighi previsti dallo strumento di trasferimento di cui all'articolo 46 del RGPD[55].

Possibili fonti di informazioni

44. L'importatore di dati dovrebbe fornirvi le fonti e le informazioni pertinenti relative al paese terzo in cui è stabilito e alle leggi e alle prassi vigenti applicabili al trasferimento.
45. Voi e l'importatore potete completare la vostra valutazione con informazioni ottenute da fonti come quelle elencate a titolo esemplificativo nell'allegato 3.
46. Oltre al quadro giuridico del paese terzo applicabile al trasferimento, le fonti e le informazioni devono essere pertinenti, oggettive, attendibili, verificabili e disponibili al pubblico o altrimenti accessibili per determinare se il vostro strumento di trasferimento di cui all'articolo 46 possa essere effettivamente applicato[56] e dovrete valutare e documentare che siano tali.

Pertinenti: le informazioni devono essere pertinenti per il trasferimento specifico e/o l'importatore, nonché per la loro conformità ai requisiti previsti dal diritto dell'UE e dallo strumento di trasferimento di cui all'articolo 46 del RGPD, senza essere eccessivamente generiche o astratte.

Informazioni oggettive: sono informazioni suffragate da prove empiriche basate sulle conoscenze acquisite in passato, e non ipotesi su eventi e rischi potenziali.

Attendibili: l'esportatore e l'importatore devono valutare obiettivamente l'attendibilità della fonte di informazioni e delle informazioni stesse, oltre a valutarle separatamente.

Verificabili: le informazioni e le conclusioni dovrebbero essere verificabili o confrontabili con altri tipi di informazioni o fonti, nel quadro di una valutazione generale, per consentire inoltre all'autorità di controllo o giudiziaria competente di verificare l'oggettività e l'attendibilità di tali informazioni, se necessario.

Informazioni disponibili al pubblico o altrimenti accessibili: le informazioni dovrebbero preferibilmente essere pubbliche o almeno accessibili

per facilitare la verifica dei criteri di cui sopra e garantire la possibilità di condividerli con autorità di controllo, autorità giudiziarie e, in ultima analisi, con gli interessati.

47. Potreste tenere conto altresì dell'esperienza documentata dell'importatore con riguardo a casi precedenti e pertinenti di richieste di accesso pervenute da autorità pubbliche nel paese terzo. Potrete avvalervi dell'esperienza dell'importatore in quanto fonte ulteriore di informazioni solo se il quadro giuridico del paese terzo non vieta all'importatore di fornire informazioni su richieste di comunicazione da parte di autorità pubbliche o sull'assenza di tali richieste (e dovreste anche documentare tale valutazione). Occorre comunque considerare che l'assenza di casi precedenti di richieste ricevute dall'importatore non può mai essere ritenuta, di per sé, un fattore decisivo in merito all'efficacia dello strumento di trasferimento di cui all'articolo 46 del RGPD, tale da consentire di procedere con il trasferimento senza adottare misure supplementari. Potrete prendere in considerazione queste informazioni, unitamente ad altre categorie di informazioni ottenute da altre fonti, nell'ambito della vostra valutazione generale delle norme e delle prassi del paese terzo in relazione al vostro trasferimento. L'esperienza pertinente e documentata dell'importatore dovrebbe essere corroborata, e non contraddetta, da informazioni pertinenti, oggettive, attendibili, verificabili e disponibili al pubblico o altrimenti accessibili sull'applicazione pratica della normativa pertinente (per esempio sull'esistenza o sull'assenza di richieste di accesso ricevute da altri soggetti che operano nello stesso settore e/o in relazione a dati personali trasferiti di natura analoga[57] e/o in merito all'applicazione concreta della normativa, ad esempio giurisprudenza e relazioni a cura di organi di vigilanza indipendenti).

Risultati della vostra valutazione

48. Dovete condurre questa valutazione generale della legislazione e delle prassi del paese terzo del vostro importatore, applicabili al trasferimento, con la dovuta diligenza e documentarla accuratamente. Le vostre autorità di controllo e/o giudiziarie competenti potrebbero richiederla e ritenervi responsabili per qualsiasi decisione da voi presa su tale base[58].

49. La vostra valutazione può in ultima analisi indicare che lo strumento di trasferimento di cui all'articolo 46 del RGPD su cui fate affidamento:

- garantisce in modo efficace che i dati personali trasferiti godano nel paese terzo di un livello di protezione sostanzialmente equivalente a quello garantito nel SEE. La legislazione e le prassi del paese terzo applicabili al trasferimento permettono all'importatore di dati di rispettare gli obblighi previsti dallo strumento di trasferimento prescelto. Dovreste procedere a una nuova valutazione a intervalli adeguati o quando emergono cambiamenti significativi (cfr. sesto passo); oppure
- non garantisce in modo efficace un livello di protezione sostanzialmente equivalente. L'importatore di dati non può adempiere i suoi obblighi, a causa

della legislazione e/o delle prassi del paese terzo applicabili al trasferimento che non sono conformi alle norme dell'UE in materia di diritti e libertà fondamentali e alla necessità e proporzionalità delle restrizioni ivi contemplate per salvaguardare obiettivi legittimi di pubblico interesse. La CGUE ha sottolineato che, qualora gli strumenti di trasferimento di cui all'articolo 46 del RGPD non siano sufficienti, spetta all'esportatore di dati mettere in atto misure supplementari efficaci o non trasferire i dati personali[59].

Esempio:

Contesto

La CGUE ha ritenuto che l'articolo 702 del Foreign Intelligence Surveillance Act (FISA) statunitense non rispetti le garanzie minime derivanti dal principio di proporzionalità ai sensi del diritto dell'Unione e non possa essere considerato limitato allo stretto necessario. Ciò significa che il livello di protezione dei programmi autorizzati dall'articolo 702 della FISA non è sostanzialmente equivalente alle garanzie richieste dal diritto dell'Unione.

Valutazione

Se la valutazione della legislazione statunitense pertinente vi induce a ritenere che il vostro trasferimento possa rientrare nell'ambito di applicazione dell'articolo 702 della FISA, ma non siete certi che rientri in concreto nel suo campo di applicazione, potete decidere di:

1. interrompere il trasferimento;
2. adottare misure supplementari adeguate che garantiscano in modo efficace un livello di protezione per i dati trasferiti sostanzialmente equivalente a quello garantito nel SEE; oppure
3. considerare altre informazioni oggettive, attendibili, pertinenti, verificabili e preferibilmente disponibili al pubblico (comprese eventualmente informazioni che vi ha fornito l'importatore di dati) per precisare in concreto il campo di applicazione dell'articolo 702 della FISA nei confronti del vostro trasferimento. Queste informazioni dovrebbero fornire risposte ad alcune domande pertinenti, quali:

- le informazioni disponibili al pubblico dimostrano l'esistenza di un divieto legale di fornire informazioni su una specifica richiesta di accesso a dati ricevuti e la presenza di ampie limitazioni alla possibilità di fornire informazioni generali su richieste di accesso a dati ricevuti o sull'assenza di tali richieste?
- L'importatore di dati ha confermato di avere ricevuto in passato richieste di accesso ai dati da parte di autorità pubbliche statunitensi? Oppure l'importatore di dati ha confermato di non avere ricevuto in passato richieste di accesso ai dati da parte di autorità pubbliche statunitensi e che gli è consentito fornire informazioni su tali richieste o sulla loro assenza?
- Le informazioni disponibili al pubblico ottenute sulla giurisprudenza statunitense e sulle relazioni a cura di organi di vigilanza, organizzazioni

della società civile e istituzioni accademiche[60] indicano che importatori di dati operanti nello stesso settore del vostro importatore hanno ricevuto in passato richieste di accesso a dati trasferiti di natura analoga?

Le risposte a queste domande, da voi ottenute per mezzo della valutazione generale, vi inducono a concludere che:

- l'articolo 702 della FISA si applica in concreto al vostro trasferimento e, pertanto, incide sull'efficacia del vostro strumento di trasferimento di cui all'articolo 46 del RGPD. Di conseguenza, se desiderate procedere con il trasferimento, dovete valutare, ove opportuno in collaborazione con l'importatore, la possibilità di adottare misure supplementari che garantiscano in modo efficace un livello di protezione per i dati trasferiti sostanzialmente equivalente a quello garantito nel SEE. Qualora non possiate individuare misure supplementari efficaci, non dovete trasferire i dati personali;

  oppure

- l'articolo 702 della FISA non si applica in concreto al vostro trasferimento e, pertanto, non incide sull'efficacia del vostro strumento di trasferimento di cui all'articolo 46 del RGPD. Potete quindi procedere con il trasferimento senza adottare misure supplementari.

2.4 QUARTO PASSO: ADOZIONE DI MISURE SUPPLEMENTARI

50. Se la valutazione di cui al terzo passo ha indicato che lo strumento di trasferimento di cui all'articolo 46 del RGPD non è efficace, dovrete considerare, se del caso in collaborazione con l'importatore, l'eventuale esistenza di misure supplementari che, aggiunte alle garanzie contenute negli strumenti di trasferimento, potrebbero garantire che i dati trasferiti godano, nel paese terzo, di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE[61]. Le «misure supplementari» integrano per definizione le garanzie già previste dallo strumento di trasferimento di cui all'articolo 46 del RGPD e qualsiasi altro requisito di sicurezza applicabile (per esempio misure tecniche di sicurezza) previste dal RGPD[62].

51. Dovete individuare caso per caso quali misure supplementari potrebbero essere efficaci per i trasferimenti verso un determinato paese terzo quando utilizzate uno specifico strumento di trasferimento di cui all'articolo 46 del RGPD. Non è necessario che ripetiate la valutazione ogni volta che effettuate lo stesso trasferimento di una specifica tipologia di dati verso lo stesso paese terzo. Alcuni dei dati per cui è previsto il trasferimento potrebbero richiedere misure supplementari, mentre per altri dati ciò potrebbe non essere necessario (considerando l'applicazione formale e/o concreta della legislazione del paese terzo). Potrete basarvi sulle precedenti valutazioni e conclusioni di cui al primo, secondo e terzo passo e verificare, sulla base di quelle conclusioni, la potenziale efficacia delle misure supplementari nel garantire il livello di protezione richiesto.

52. In linea di principio, le misure supplementari possono avere carattere contrattuale, tecnico o organizzativo. La combinazione di misure diverse che si integrino e supportino a vicenda può migliorare il livello di protezione e può quindi contribuire a raggiungere gli standard dell'Unione.

53. Le misure contrattuali e organizzative, da sole, non riescono in genere a evitare l'accesso ai dati personali da parte delle autorità pubbliche del paese terzo in forza di una legislazione e/o di prassi problematiche[63]. Vi saranno infatti situazioni in cui solo misure tecniche adeguatamente attuate potrebbero impedire o rendere inefficace l'accesso ai dati personali da parte delle autorità pubbliche dei paesi terzi, in particolare a fini di sorveglianza[64]. In tali situazioni, le misure contrattuali o organizzative possono integrare le misure tecniche e rafforzare il livello generale di protezione dei dati, ad esempio introducendo controlli ed eliminando automatismi in relazione ai tentativi delle autorità pubbliche di accedere ai dati in modo non conforme alle norme dell'Unione.

54. In collaborazione con l'importatore di dati, se del caso, potete consultare il seguente elenco (non esaustivo) di fattori al fine di individuare quali misure supplementari sarebbero più efficaci per proteggere i dati trasferiti dalle richieste di accesso agli stessi da parte di autorità pubbliche in forza di una legislazione problematica applicata in concreto al trasferimento:

- formato dei dati da trasferire (ad esempio in chiaro/dati pseudonimizzati o cifrati);
- natura dei dati (per esempio, nel SEE le categorie di dati contemplate dagli articoli 9 e 10 del RGPD godono di un livello di protezione superiore)[65];
- lunghezza e complessità della catena di trattamento dei dati, numero di soggetti coinvolti nel trattamento e rapporti intercorrenti (ad esempio se i trasferimenti coinvolgono più titolari del trattamento ovvero titolari e responsabili del trattamento, oppure se sono coinvolti responsabili del trattamento che trasferiranno i dati da voi all'importatore dei dati, considerando le relative disposizioni loro applicabili ai sensi della legislazione del paese terzo di destinazione)[66];
- tecnica o parametri dell'applicazione pratica nel paese terzo riscontrati nel corso del terzo passo;
- possibilità che i dati siano oggetto di trasferimenti successivi, all'interno dello stesso paese terzo o anche verso altri paesi terzi (ad esempio coinvolgimento di sub-responsabili del trattamento dell'importatore dei dati)[67].

Esempi di misure supplementari

55. Alcuni esempi di misure tecniche, contrattuali e organizzative che potrebbero essere prese in considerazione, ove non siano già incluse nello strumento di trasferimento utilizzato di cui all'articolo 46 del RGPD, sono disponibili negli elenchi non esaustivi di cui all'allegato 2.

***

56. Se avete messo in atto misure supplementari efficaci che, combinate con lo strumento di trasferimento di cui all'articolo 46 del RGPD prescelto, raggiungono un livello di protezione sostanzialmente equivalente al livello di protezione garantito all'interno del SEE, potete procedere con i vostri trasferimenti.

57. Qualora non siate in grado di individuare o attuare misure supplementari efficaci che garantiscano che i dati personali trasferiti godano di un livello di protezione sostanzialmente equivalente[68], non dovete iniziare a trasferire i dati personali verso il paese terzo interessato sulla base dello strumento di trasferimento di cui all'articolo 46 del RGPD su cui fate affidamento. Se state già effettuando trasferimenti, siete tenuti a sospendere o a porre fine al trasferimento dei dati personali[69]. In conformità alle garanzie previste dallo strumento di trasferimento di cui all'articolo 46 del RGPD su cui fate affidamento, i dati che avete già trasferito a tale paese terzo e le relative copie devono esservi restituiti o distrutti interamente dall'importatore[70].

Esempio:

La legge del paese terzo vieta le misure supplementari da voi individuate (ad esempio vieta l'uso della cifratura) o ne impedisce in altro modo l'efficacia. Non dovete iniziare a trasferire i dati personali verso questo paese, oppure dovete interrompere i trasferimenti in corso verso questo paese.

58. L'autorità di controllo competente può imporre altre misure correttive (ad esempio una sanzione) se avviate o continuate il trasferimento sebbene non possiate dimostrare un livello di protezione sostanzialmente equivalente nel paese terzo.

2.5 QUINTO PASSO: PASSAGGI PROCEDURALI SE AVETE INDIVIDUATO MISURE SUPPLEMENTARI EFFICACI

59. I passaggi procedurali da adottare nel caso in cui abbiate individuato misure supplementari efficaci da mettere in atto possono essere diversi a seconda dello strumento di trasferimento di cui all'articolo 46 del RGPD che state utilizzando o che prevedete di utilizzare.

2.5.1 CLAUSOLE TIPO DI PROTEZIONE DEI DATI (ARTICOLO 46, PARAGRAFO 2, LETTERE C) E D), DEL RGPD)

60. Quando intendete mettere in atto misure supplementari in aggiunta alle clausole contrattuali tipo, non è necessario richiedere un'autorizzazione all'autorità di controllo competente per aggiungere questo tipo di clausole o garanzie supplementari, a condizione che le misure supplementari individuate non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo e siano sufficienti a garantire che il livello di protezione previsto

dal RGPD non sia pregiudicato[71]. L'esportatore e l'importatore di dati devono garantire che le clausole aggiuntive non possano essere interpretate in alcun modo che comporti limitazioni dei diritti e degli obblighi previsti dalle clausole contrattuali tipo o che comunque riduca il livello di protezione dei dati. Dovete essere in grado di dimostrare quanto sopra, compresa l'inequivocabilità di tutte le clausole, ai sensi del principio di responsabilizzazione e dell'obbligo di fornire un livello sufficiente di protezione dei dati. Le autorità di controllo competenti hanno il potere di esaminare tali clausole supplementari se necessario (ad esempio in caso di reclamo o a seguito di indagine d'ufficio).

61. Qualora intendiate modificare le clausole tipo di protezione dei dati o qualora le misure supplementari aggiunte «contraddicano» direttamente o indirettamente le clausole contrattuali tipo, si riterrà che non vi facciate più affidamento[72] e dovrete chiedere un'autorizzazione all'autorità di controllo competente ai sensi dell'articolo 46, paragrafo 3, lettera a), del RGPD.

2.5.2 NORME VINCOLANTI D'IMPRESA (BCR) (ARTICOLO 46, PARAGRAFO 2, LETTERA B), DEL RGPD)

62. Il ragionamento della sentenza Schrems II si applica anche ad altri strumenti di trasferimento di cui all'articolo 46, paragrafo 2, del RGPD, poiché tutti questi strumenti sono fondamentalmente di natura contrattuale, per cui le garanzie previste e gli impegni assunti dalle parti non possono vincolare le autorità pubbliche di paesi terzi[73].
63. La sentenza Schrems II è rilevante per i trasferimenti di dati personali sulla base di norme vincolanti d'impresa (BCR), poiché le normative di paesi terzi possono influire sulla protezione fornita da tali strumenti.
64. Tutti gli impegni che devono essere inclusi saranno riportati nei criteri di riferimento WP256/257 aggiornati[74] cui tutti i gruppi facenti affidamento su BCR ai fini dei trasferimenti di dati dovranno allineare le loro BCR vigenti e future.
65. La Corte ha sottolineato che è responsabilità dell'esportatore e dell'importatore dei dati verificare il rispetto, nel paese terzo interessato, del livello di protezione richiesto dal diritto dell'Unione, al fine di determinare se le garanzie previste dalle clausole contrattuali tipo o dalle norme vincolanti d'impresa possano essere rispettate nella pratica. In caso contrario, si deve accertare che sia possibile prevedere misure supplementari atte a garantire un livello di protezione sostanzialmente equivalente a quello in vigore nel SEE e che il diritto o la prassi del paese terzo non interferiscano con tali misure supplementari in modo da impedirne l'efficacia.

2.5.3 CLAUSOLE CONTRATTUALI AD HOC (ARTICOLO 46, PARAGRAFO 3, LETTERA A), DEL RGPD)

66. Il ragionamento della sentenza Schrems II si applica anche ad altri strumenti di trasferimento di cui all'articolo 46, paragrafo 2, del RGPD, poiché tutti

questi strumenti sono fondamentalmente di natura contrattuale, per cui le garanzie previste e gli impegni assunti dalle parti non possono vincolare le autorità pubbliche di paesi terzi[75]. La sentenza Schrems II è dunque rilevante per i trasferimenti di dati personali sulla base di clausole contrattuali ad hoc, poiché le normative di paesi terzi possono influire sulla protezione fornita da tali strumenti.

2.6 SESTO PASSO: RIVALUTARE A INTERVALLI APPROPRIATI

67. Dovete monitorare costantemente e, se del caso, in collaborazione con gli importatori di dati, gli sviluppi che, nel paese terzo verso cui avete trasferito i dati personali, potrebbero influenzare la vostra valutazione iniziale del livello di protezione e le decisioni che potreste aver preso di conseguenza sui trasferimenti. La responsabilizzazione è un obbligo permanente (articolo 5, paragrafo 2, del RGPD).
68. Dovreste mettere in atto meccanismi sufficientemente solidi per garantire la sospensione o la cessazione immediata dei trasferimenti qualora:

- l'importatore abbia violato o non sia in grado di onorare gli impegni assunti con lo strumento di trasferimento di cui all'articolo 46 del RGPD; oppure
- le misure supplementari non siano più efficaci in tale paese terzo.

3. CONCLUSIONI

69. Il RGPD stabilisce norme sul trattamento dei dati personali nel SEE e, in tal senso, consente la libera circolazione dei dati personali all'interno del SEE. Il capo V del regolamento disciplina i trasferimenti di dati personali verso paesi terzi e fissa un limite elevato: il trasferimento non deve pregiudicare il livello di protezione delle persone fisiche garantito dal RGPD (articolo 44 del RGPD). La sentenza C311/18 (Schrems II) della CGUE sottolinea la necessità di garantire la continuità del livello di protezione garantito dal RGPD ai dati personali trasferiti verso un paese terzo[76].
70. Per garantire un livello di protezione sostanzialmente equivalente dei vostri dati, dovete innanzitutto conoscere a fondo i vostri trasferimenti. Dovete inoltre controllare che i dati trasferiti siano adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali vengono trattati.
71. Dovete anche individuare lo strumento di trasferimento su cui fate affidamento per i vostri trasferimenti. Se lo strumento di trasferimento non è una decisione di adeguatezza, dovete verificare caso per caso se il diritto o le prassi del paese terzo di destinazione pregiudicano (oppure no) le garanzie previste dallo strumento di trasferimento di cui all'articolo 46 del RGPD nel contesto dei vostri trasferimenti. Se lo strumento di trasferimento di cui all'articolo 46 del RGPD non riesce a garantire, di per sé, un livello di protezione sostanzialmente equivalente per i dati personali da voi trasferiti, misure supplementari possono colmare la lacuna.

72. Qualora non siate in grado di individuare o attuare misure supplementari efficaci che garantiscano che i dati personali trasferiti beneficino di un livello di protezione sostanzialmente equivalente, non dovete iniziare a trasferire i dati personali verso il paese terzo interessato sulla base dello strumento di trasferimento prescelto. Se state già effettuando trasferimenti, siete tenuti a sospendere o a porre fine prontamente al trasferimento dei dati personali.
73. L'autorità di controllo competente ha il potere di sospendere o porre fine ai trasferimenti di dati personali verso il paese terzo se non è garantita la protezione dei dati trasferiti richiesta dal diritto dell'Unione, in particolare dagli articoli 45 e 46 del RGPD e dalla Carta dei diritti fondamentali.

Per il comitato europeo per la protezione dei dati
La presidente

(Andrea Jelinek)

ALLEGATO 1: DEFINIZIONI

- Per «paese terzo» si intende qualsiasi paese che non sia uno Stato membro del SEE.
- Per «SEE» si intende lo Spazio economico europeo, che comprende gli Stati membri dell'Unione europea e l'Islanda, la Norvegia e il Liechtenstein. A questi ultimi si applica il RGPD in virtù dell'accordo SEE, in particolare l'allegato XI e il protocollo 37.
- «RGPD» si riferisce al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
- «La Carta» si riferisce alla Carta dei diritti fondamentali dell'Unione europea (GU C 326 del 26.10.2012, pagg. 391-407).
- «CGUE» o «la Corte» si riferisce alla Corte di giustizia dell'Unione europea, che costituisce l'autorità giudiziaria dell'Unione europea e, in collaborazione con le corti e i tribunali degli Stati membri, garantisce l'applicazione e l'interpretazione uniformi del diritto dell'Unione.
- Per «esportatore di dati» si intende il titolare del trattamento o il responsabile del trattamento all'interno del SEE che trasferisce dati personali a un titolare del trattamento o a un responsabile del trattamento in un paese terzo.
- Per «importatore di dati» si intende il titolare del trattamento o il responsabile del trattamento in un paese terzo che riceve o ottiene accesso ai dati personali trasferiti dal SEE.
- «Strumento di trasferimento di cui all'articolo 46 del RGPD» si riferisce alle garanzie adeguate ai sensi dell'articolo 46 del RGPD che gli esportatori di dati mettono in atto quando trasferiscono dati personali verso un paese terzo, in assenza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, del RGPD. L'articolo 46, paragrafi 2 e 3, del RGPD contiene l'elenco degli strumenti di trasferimento di cui all'articolo 46 del RGPD che i titolari del trattamento e i responsabili del trattamento possono utilizzare.
- Per «clausole contrattuali tipo» si intendono le clausole standard di protezione dei dati adottate dalla Commissione europea per i trasferimenti di dati personali tra titolari del trattamento o responsabili del trattamento nel SEE e titolari del trattamento o responsabili del trattamento al di fuori del SEE. Le clausole contrattuali tipo adottate dalla Commissione europea sono uno strumento di trasferimento ai sensi dell'articolo 46, paragrafo 2, lettera c), e dell'articolo 46, paragrafo 5, del RGPD.

ALLEGATO 2: ESEMPI DI MISURE SUPPLEMENTARI

74. Le seguenti misure sono esempi di misure supplementari che è possibile prendere in considerazione quando si renda necessario (v. quarto passo) «adottare misure supplementari». L'elenco presentato non è esaustivo, ed è possibile prendere in considerazione altre misure supplementari. Sviluppi tecnologici, giuridici od organizzativi futuri potrebbero comportare la necessità di valutare nuove misure supplementari. La selezione e l'implementazione di una o più di queste misure non garantirà necessariamente e sistematicamente che il vostro trasferimento soddisfi gli standard di sostanziale equivalenza richiesti dal diritto dell'Unione. Dovreste selezionare le misure supplementari che possono garantire efficacemente tale livello di protezione per i vostri trasferimenti.
75. Qualsiasi misura supplementare può essere considerata efficace ai sensi della sentenza della CGUE «Schrems II» solo se e nella misura in cui, di per sé o in combinazione con altre, affronta le specifiche carenze individuate nella valutazione della situazione del paese terzo per quanto riguarda il diritto e le prassi di tale paese applicabili al vostro trasferimento. Se, in ultima analisi, non riuscite a garantire un livello di protezione sostanzialmente equivalente, non dovete trasferire i dati personali.
76. In qualità di titolari o di responsabili del trattamento, potreste essere già tenuti ad attuare alcune delle misure descritte nel presente allegato, ai fini della conformità al RGPD. Ciò implica la possibilità di mettere in atto misure analoghe per i dati personali trattati nel SEE che siano trasferiti a un importatore di dati coperto da una decisione di adeguatezza o verso altri paesi terzi[77].

2.1 MISURE TECNICHE

77. Questa sezione descrive in modo non esaustivo esempi di misure tecniche che possono integrare le garanzie previste dagli strumenti di trasferimento di cui all'articolo 46 del RGPD, per assicurare il rispetto del livello di protezione richiesto dal diritto dell'Unione nel contesto di un trasferimento di dati personali verso un paese terzo. Tali misure saranno particolarmente necessarie qualora la legislazione di tale paese imponga all'importatore di dati obblighi che sono in contrasto con le garanzie previste dagli strumenti di trasferimento di cui all'articolo 46 del RGPD e che sono, in particolare, in grado di pregiudicare la garanzia contrattuale di un livello di protezione sostanzialmente equivalente rispetto all'accesso a tali dati da parte delle autorità pubbliche di tale paese terzo[78].
78. Per maggiore chiarezza, questa sezione descrive in primo luogo esempi di scenari in cui determinate misure tecniche potrebbero essere efficaci per garantire un livello di protezione sostanzialmente equivalente. La sezione prosegue con alcuni scenari per i quali non sono individuate le misure tecniche atte a garantire tale livello di protezione.

Esempi di scenari relativi a casi per i quali sono individuate misure *efficaci*

79. Le misure elencate di seguito sono intese a garantire che l'accesso ai dati trasferiti da parte delle autorità pubbliche di paesi terzi non pregiudichi l'efficacia delle garanzie adeguate previste dagli strumenti di trasferimento di cui all'articolo 46 del RGPD. Tali misure sarebbero necessarie per assicurare un livello di protezione sostanzialmente equivalente a quello garantito nel SEE, anche se l'accesso delle autorità pubbliche è conforme alla legge del paese dell'importatore, qualora, in concreto, tale accesso vada al di là di quanto necessario e proporzionato in una società democratica[79]. Le misure hanno lo scopo di impedire l'accesso potenzialmente illecito impedendo alle autorità di identificare gli interessati, di dedurre informazioni che li riguardano, di individuarli in un altro contesto o di associare i dati trasferiti ad altri insiemi di dati che possono contenere, tra l'altro, identificatori online forniti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati dagli interessati in altri contesti.

80. Le autorità pubbliche dei paesi terzi possono cercare di accedere ai dati trasferiti:

a) in transito, accedendo alle linee di comunicazione utilizzate per trasmettere i dati al paese destinatario. Questo accesso può essere passivo, nel qual caso il contenuto della comunicazione, eventualmente dopo un processo di selezione, viene semplicemente copiato. L'accesso può tuttavia essere anche attivo, nel senso che le autorità pubbliche si interpongono nel processo di comunicazione non solo leggendo il contenuto, ma anche manipolando o sopprimendo parti di esso;

b) durante la custodia da parte di un destinatario dei dati, accedendo direttamente alle strutture di trattamento o chiedendo al destinatario dei dati di localizzarli, estrarre i dati di interesse e consegnarli alle autorità.

81. In questa sezione vengono presi in considerazione gli scenari in cui vengono applicate misure efficaci in entrambi i casi. L'applicazione di misure supplementari di diverso genere può risultare sufficiente nelle circostanze specifiche di un determinato trasferimento se la legislazione del paese destinatario prevede un solo tipo di accesso. È quindi necessario che l'esportatore di dati analizzi attentamente, con il supporto dell'importatore di dati, gli obblighi che incombono a quest'ultimo.

> A titolo di esempio, gli importatori di dati statunitensi che rientrano nel campo di applicazione del titolo 50 U.S.C. § 1881 bis (sezione 702 della FISA) hanno l'obbligo diretto di concedere l'accesso a dati personali importati che sono in loro possesso, custodia o controllo, o di consegnarli. Ciò può estendersi a qualsiasi chiave crittografica necessaria per rendere i dati intelligibili.

82. Gli scenari descrivono circostanze specifiche e le misure adottate a titolo di esempio. Qualsiasi modifica degli scenari può portare a conclusioni diverse.

Gli scenari si riferiscono a situazioni in cui si è concluso preliminarmente che occorrono misure supplementari, vale a dire situazioni ove, in concreto, la legislazione problematica del paese terzo venga applicata al trasferimento in questione.

83. I titolari del trattamento possono essere tenuti ad applicare alcune o la totalità delle misure qui descritte indipendentemente dal livello di protezione previsto dalle norme applicabili all'importatore di dati, poiché esse sono necessarie per conformarsi agli articoli 25 e 32 del RGPD nelle circostanze concrete del trasferimento. In altre parole, gli esportatori possono essere tenuti ad attuare le misure descritte nel presente documento anche se i rispettivi importatori di dati sono coperti da una decisione di adeguatezza, nello stesso modo in cui titolari e responsabili del trattamento possono essere tenuti ad attuarle quando i dati sono trattati all'interno del SEE.

Caso d'uso 1: conservazione dei dati per il backup e per altri scopi che non richiedono l'accesso ai dati in chiaro

84. Un esportatore di dati utilizza un fornitore di servizi di hosting in un paese terzo per conservare dati personali, ad esempio a scopo di backup.

Se

1. i dati personali sono trattati con una crittografia forte prima della trasmissione e l'identità dell'importatore è verificata,
2. l'algoritmo di cifratura e la sua parametrizzazione (ad esempio la lunghezza della chiave o la modalità di funzionamento, se applicabili) sono conformi allo stato dell'arte e possono essere considerati solidi rispetto alla crittoanalisi effettuata dalle autorità pubbliche del paese destinatario, tenendo conto delle risorse e delle capacità tecniche (ad esempio potenza di calcolo per attacchi di forza bruta) a loro disposizione[80],
3. l'efficacia della crittografia e la lunghezza della chiave tengono conto del periodo di tempo specifico durante il quale la riservatezza dei dati personali cifrati deve essere preservata[81],
4. l'algoritmo di cifratura è applicato correttamente da un software adeguatamente aggiornato e senza vulnerabilità note, la cui conformità alle specifiche dell'algoritmo scelto è stata verificata, ad esempio mediante certificazione,
5. le chiavi sono gestite in modo affidabile (generate, amministrate, conservate, se del caso, collegate all'identità di un destinatario e revocate)[82], e
6. le chiavi sono conservate esclusivamente sotto il controllo dell'esportatore di dati, o di un soggetto incaricato dall'esportatore nel SEE o in una giurisdizione che offre un livello di protezione sostanzialmente equivalente a quello garantito all'interno del SEE,

l'EDPB ritiene allora che la cifratura eseguita costituisca un'efficace misura supplementare.

Caso d'uso 2: trasferimento di dati pseudonimizzati

85. Un esportatore di dati pseudonimizza, in primo luogo, i dati in suo possesso e poi li trasferisce verso un paese terzo per analizzarli, ad esempio a scopo di ricerca.

    Se

    1. l'esportatore trasferisce i dati personali trattati in modo tale che non possano più essere attribuiti a un determinato interessato, né essere utilizzati per individuare l'interessato in un gruppo più ampio senza l'impiego di informazioni aggiuntive[83],
    2. tali informazioni aggiuntive sono detenute esclusivamente dall'esportatore di dati e conservate separatamente in uno Stato membro o in un paese terzo da un soggetto incaricato dall'esportatore nel SEE o in una giurisdizione che offre un livello di protezione sostanzialmente equivalente a quello garantito all'interno del SEE,
    3. la divulgazione o l'uso non autorizzato di tali informazioni aggiuntive sono impediti da adeguate misure di sicurezza tecniche e organizzative, si garantisce che l'esportatore di dati mantiene il controllo esclusivo dell'algoritmo o del repository che consente la re-identificazione utilizzando le informazioni aggiuntive, e
    4. il titolare del trattamento ha stabilito, mediante un'analisi approfondita dei dati in questione, tenendo conto di ogni informazione che le autorità pubbliche del paese destinatario potrebbero presumibilmente possedere e utilizzare, che i dati personali pseudonimizzati non possono essere attribuiti a una persona fisica identificata o identificabile, anche se incrociati con tali informazioni,

    l'EDPB ritiene allora che la pseudonimizzazione eseguita costituisca un'efficace misura supplementare.

86. Si noti che in molte situazioni, fattori specifici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di una persona fisica, la sua ubicazione o la sua interazione con un servizio basato su Internet in determinati momenti[84] possono consentirne l'identificazione anche se il suo nome, indirizzo o altri identificativi semplici sono omessi.

87. Ciò vale in particolare quando i dati riguardano l'utilizzo di servizi d'informazione (orario di accesso, sequenza delle funzionalità a cui è stato effettuato l'accesso, caratteristiche del dispositivo utilizzato, ecc.). Tali servizi potrebbero essere, come per l'importatore di dati personali, soggetti all'obbligo di concedere l'accesso alle stesse autorità pubbliche nella propria giurisdizione, che potranno così disporre di dati relativi all'utilizzo di tali servizi d'informazione da parte della persona o delle persone oggetto di attenzione.

88. Inoltre, dato che l'uso di alcuni servizi d'informazione è pubblico per natura, o che tali servizi sono utilizzabili da parte di soggetti che dispongono di notevoli risorse, i titolari del trattamento dovranno prestare particolare attenzione, considerando che le autorità pubbliche nella propria giurisdizione

potrebbero essere in possesso di dati sull'uso dei servizi d'informazione da parte di una persona oggetto della loro attenzione.

89. Se, nel corso della pseudonimizzazione, gli attributi contenuti nei dati personali vengono trasformati per mezzo di un algoritmo crittografico, si applicano gli orientamenti di cui alle note 80 e 81. Si raccomanda quindi di rinunciare all'uso esclusivo della crittografia e di applicare le trasformazioni in base ai meccanismi di consultazione (look-up) delle tabelle.

Caso d'uso 3: cifratura dei dati per proteggerli dall'accesso delle autorità pubbliche del paese terzo dell'importatore quando transitano dall'esportatore all'importatore

90. Un esportatore di dati desidera trasferire dati verso una destinazione in cui il diritto e/o le prassi consentono l'accesso delle autorità pubbliche ai dati mentre questi ultimi transitano dal paese dell'esportatore a quello di destinazione.

    Se

    1. un esportatore di dati trasferisce i dati personali a un importatore di dati in una giurisdizione in cui il diritto e/o le prassi consentono alle autorità pubbliche di accedere ai dati mentre questi vengono trasportati su Internet verso questo paese terzo senza le garanzie essenziali europee riguardanti tale accesso, viene utilizzata la cifratura del trasporto, per la quale si garantisce che i protocolli di cifratura impiegati sono conformi allo stato dell'arte e forniscono una protezione efficace contro gli attacchi attivi e passivi con risorse notoriamente a disposizione delle autorità pubbliche del paese terzo,
    2. le parti coinvolte nella comunicazione si accordano su un'autorità o un'infrastruttura di certificazione a chiave pubblica affidabile,
    3. vengono utilizzate misure specifiche di protezione conformi allo stato dell'arte contro gli attacchi attivi e passivi all'interno dei sistemi di invio e di ricezione che permettono la cifratura del trasporto, tra cui test per rilevare le vulnerabilità del software e possibili backdoor,
    4. nel caso in cui la cifratura del trasporto non fornisca di per sé una sicurezza adeguata a causa di esperienze di vulnerabilità dell'infrastruttura o del software utilizzato, i dati personali vengono anche cifrati end-to-end sul livello dell'applicazione utilizzando metodi di cifratura conformi allo stato dell'arte,
    5. l'algoritmo di cifratura e la sua parametrizzazione (ad esempio la lunghezza della chiave o la modalità di funzionamento, se applicabili) sono conformi allo stato dell'arte e possono essere considerati solidi rispetto all'analisi di cifratura effettuata dalle autorità pubbliche quando i dati sono in transito verso il paese terzo, tenendo conto delle risorse e delle capacità tecniche (ad esempio potenza di calcolo per attacchi di forza bruta) a loro disposizione (cfr. la precedente nota 80)[85],
    6. l'efficacia della crittografia tiene conto del periodo di tempo specifico duran-

te il quale la riservatezza dei dati personali cifrati deve essere preservata,

7. l'algoritmo di cifratura è applicato correttamente da un software adeguatamente aggiornato e senza vulnerabilità note, la cui conformità alle specifiche dell'algoritmo scelto è stata verificata, ad esempio mediante certificazione,
8. le chiavi sono gestite in modo affidabile (generate, amministrate, conservate, se del caso, collegate all'identità del destinatario previsto, e revocate), dall'esportatore o da un soggetto di fiducia dell'esportatore in una giurisdizione che offre un livello di protezione sostanzialmente equivalente,

l'EDPB ritiene allora che la cifratura del trasporto, ove del caso in combinazione con la cifratura dei contenuti end-to-end, costituisca un'efficace misura supplementare.

Caso d'uso 4: destinatario protetto

91. Un esportatore di dati trasferisce dati personali a un importatore di dati in un paese terzo specificamente protetto dalla legge di tale paese, ad esempio per fornire congiuntamente cure mediche a un paziente o servizi legali a un cliente.

Se

1. la legislazione del paese terzo esclude che l'importatore di dati residente possa essere interessato da forme di accesso ai dati da quest'ultimo detenuti per la finalità specifica potenzialmente in violazione delle garanzie previste, ad esempio in virtù di un obbligo di segreto professionale che si applica all'importatore di dati,
2. tale esclusione si estende a tutte le informazioni in possesso dell'importatore di dati che possono essere utilizzate per eludere la protezione delle informazioni privilegiate (chiavi cifrate, password, altre credenziali, ecc.),
3. l'importatore di dati non si avvale dei servizi di un responsabile del trattamento in modo tale da consentire alle autorità pubbliche di accedere ai dati in possesso di quest'ultimo, né inoltra i dati a un altro soggetto che non gode delle tutele di cui sopra, sulla base degli strumenti di trasferimento di cui all'articolo 46 del RGPD,
4. i dati personali sono cifrati prima di essere trasmessi con un metodo conforme allo stato dell'arte che garantisce che la decifrazione non sarà possibile senza la conoscenza della chiave di decifrazione (cifratura end-to-end) per tutto il tempo in cui i dati devono essere protetti,
5. la chiave di decifrazione è in custodia esclusiva dell'importatore dei dati protetto nonché, eventualmente, dell'esportatore stesso o di un altro soggetto incaricato dall'esportatore che è situato nel SEE o in un territorio che offre un livello di protezione sostanzialmente equivalente a quello garantito all'interno del SEE, ed è opportunamente protetta contro l'uso o la divulgazione non autorizzati mediante misure tecniche e organizzative conformi allo stato dell'arte, e
6. l'esportatore di dati ha stabilito in modo affidabile che la chiave di cifratu-

ra che intende utilizzare corrisponde alla chiave di decifrazione in possesso del destinatario,

l'EDPB ritiene allora che la cifratura del trasporto fornisca un'efficace misura supplementare.

Caso d'uso 5: trattamento frazionato o multilaterale

92. L'esportatore di dati desidera che i dati personali siano trattati congiuntamente da due o più responsabili del trattamento indipendenti situati in Stati diversi senza rivelare loro il contenuto dei dati. Prima della trasmissione, suddivide i dati in modo tale che nessun elemento ricevuto da un singolo responsabile del trattamento sia sufficiente per ricostruire i dati personali in tutto o in parte. L'esportatore di dati riceve il risultato del trattamento separatamente da ciascuno dei responsabili e fonde gli elementi ricevuti per arrivare al risultato finale sotto forma di dati personali o di aggregati di dati.

Se

1. l'esportatore di dati tratta i dati personali in modo tale che essi siano suddivisi in due o più parti, ciascuna delle quali non è interpretabile né può essere attribuita a un determinato interessato senza l'utilizzo di informazioni aggiuntive,
2. ciascuna parte viene trasferita a un distinto responsabile del trattamento situato in un diverso Stato,
3. i responsabili del trattamento hanno la possibilità di trattare i dati congiuntamente, ad esempio mediante un calcolo sicuro a più parti (*multi-party computation*), in modo che non venga rivelata a nessuno di loro alcuna informazione che non possedessero già prima del calcolo,
4. l'algoritmo utilizzato per il calcolo condiviso è sicuro rispetto ad avversari attivi,
5. il titolare del trattamento ha stabilito, mediante un'analisi approfondita dei dati in questione, tenendo conto delle informazioni mancanti che le autorità pubbliche dei paesi destinatari potrebbero presumibilmente possedere e utilizzare, che i dati personali trasmessi ai responsabili del trattamento non possono essere attribuiti a una persona fisica identificata o identificabile, anche se incrociati con tali informazioni,
6. non vi sono evidenze di collaborazioni tra le autorità pubbliche degli Stati in cui operano rispettivamente i responsabili del trattamento tali da consentire alle suddette autorità di accedere a tutti i set di dati personali in possesso dei responsabili del trattamento e di ricostituire e sfruttare il contenuto dei dati personali in chiaro secondo modalità tali per cui ciò non rispetterebbe l'essenza dei diritti e delle libertà fondamentali degli interessati. Analogamente, nessuna delle autorità pubbliche in nessuno di tali Stati dovrebbe avere il potere di accedere ai dati personali detenuti dai responsabili del trattamento,

l'EDPB ritiene allora che il trattamento eseguito in modalità frazionata fornisca un'efficace misura supplementare.

Esempi di scenari relativi a casi per i quali non sono individuate misure *efficaci*

93. Le misure descritte di seguito non sarebbero efficaci in alcuni scenari per garantire un livello di protezione sostanzialmente equivalente dei dati trasferiti verso il paese terzo. Pertanto, non si qualificherebbero come misure supplementari adeguate.

Caso d'uso 6: trasferimento a fornitori di servizi cloud o ad altri responsabili del trattamento che richiedono l'accesso ai dati in chiaro

94. Un esportatore di dati trasferisce dati personali, sia mediante trasmissione elettronica sia rendendoli disponibili a un fornitore di servizi cloud o a un altro responsabile del trattamento per far trattare i dati personali secondo le sue istruzioni in un paese terzo (ad esempio per fornire assistenza tecnica o effettuare qualsiasi tipo di trattamento sul cloud) e tali dati non sono - o non possono essere - pseudonimizzati come descritto nel caso d'uso 2 né cifrati come descritto nel caso d'uso 1, perché il trattamento richiede l'accesso ai dati in chiaro.

    Se

    1. il titolare del trattamento trasferisce i dati personali a un fornitore di servizi cloud o a un altro responsabile del trattamento,
    2. il fornitore di servizi cloud o altro responsabile del trattamento deve accedere ai dati in chiaro per eseguire il compito assegnato, e
    3. il potere riconosciuto alle autorità pubbliche del paese destinatario di accedere ai dati trasferiti in questione va oltre quanto necessario e proporzionato in una società democratica qualora, in concreto, la legislazione problematica del paese terzo si applichi ai trasferimenti in questione (cfr. terzo passo)[86],

    l'EDPB, considerato l'attuale stato dell'arte, non è in grado di prevedere una misura tecnica efficace per impedire che tale accesso violi i diritti fondamentali degli interessati. L'EDPB non esclude che ulteriori sviluppi tecnologici possano offrire misure in grado di conseguire gli scopi commerciali previsti, senza richiedere l'accesso in chiaro.

95. Negli scenari indicati, in cui dati personali non cifrati sono tecnicamente necessari per la fornitura del servizio da parte del responsabile del trattamento, la cifratura del trasporto e la cifratura dei dati a riposo, anche congiuntamente, non costituiscono una misura supplementare che garantisce un livello di protezione sostanzialmente equivalente se l'importatore dei dati è in possesso delle chiavi crittografiche.

Caso d'uso 7: trasferimento di dati personali per scopi commerciali, anche tramite accesso remoto

96. Un esportatore di dati trasferisce i dati personali a soggetti in un paese terzo affinché siano utilizzati per scopi commerciali condivisi, sia mediante trasmissione elettronica sia rendendoli disponibili per l'accesso remoto da parte dell'importatore, e tali dati non sono (o non possono essere) pseudonimizzati come descritto nel caso d'uso 2 né cifrati come descritto nel caso d'uso 1, perché il trattamento richiede l'accesso ai dati in chiaro. Una situazione tipica è quella in cui un titolare del trattamento o un responsabile del trattamento stabilito nel territorio di uno Stato membro trasferisce dati personali a un titolare del trattamento o a un responsabile del trattamento in un paese terzo appartenente allo stesso gruppo di imprese o a un gruppo di imprese che esercita un'attività economica comune. L'importatore di dati può, ad esempio, utilizzare i dati ricevuti per fornire servizi di gestione del personale all'esportatore di dati, e per far ciò ha bisogno di dati relativi alle risorse umane, o per comunicare con i clienti dell'esportatore di dati che vivono nell'Unione europea tramite telefono o e-mail.

    Se

    1. L'esportatore di dati trasferisce dati personali a un importatore di dati in un paese terzo rendendoli disponibili in un sistema informatico in modo da consentire all'importatore l'accesso diretto ai dati di sua scelta, oppure trasferendoli direttamente, singolarmente o in blocco, mediante l'uso di un servizio di comunicazione,
    2. l'importatore[87] tratta i dati in chiaro nel paese terzo (anche per i propri scopi, nel caso in cui sia un titolare del trattamento),
    3. il potere riconosciuto alle autorità pubbliche del paese destinatario di accedere ai dati trasferiti va oltre quanto necessario e proporzionato in una società democratica qualora, in concreto, la legislazione problematica del paese terzo si applichi ai trasferimenti in questione (cfr. terzo passo),

    l'EDPB non è in grado di prevedere una misura tecnica efficace per impedire che tale accesso violi i diritti fondamentali degli interessati.

97. Negli scenari indicati, in cui dati personali non cifrati sono tecnicamente necessari per la fornitura del servizio da parte del responsabile del trattamento, la cifratura del trasporto e la cifratura dei dati a riposo, anche congiuntamente, non costituiscono una misura supplementare che garantisce un livello di protezione sostanzialmente equivalente se l'importatore dei dati è in possesso delle chiavi crittografiche.

2.2 MISURE CONTRATTUALI SUPPLEMENTARI

98. Queste misure consisteranno generalmente in impegni contrattuali[88] unilaterali, bilaterali o multilaterali[89]. Se viene utilizzato uno strumento di trasferimento di cui all'articolo 46 del RGPD, nella maggior parte dei casi esso conterrà già una serie di impegni (per lo più contrattuali) per l'esportatore e

l'importatore dei dati, volti a tutelare i dati personali[90].

99. In alcune situazioni, tali misure possono integrare e rafforzare le garanzie che lo strumento di trasferimento e la legislazione pertinente del paese terzo possono fornire, quando, tenuto conto delle circostanze del trasferimento, essi non soddisfano tutte le condizioni necessarie per assicurare un livello di protezione sostanzialmente equivalente a quello garantito all'interno del SEE. Alla luce della natura delle misure contrattuali, che generalmente non possono vincolare le autorità di tale paese terzo quando queste ultime non sono parti del contratto[91], è possibile che tali misure debbano spesso essere combinate con altre misure tecniche e organizzative per fornire il livello di protezione dei dati richiesto. La selezione e l'attuazione di una o più di queste misure non garantirà necessariamente e sistematicamente che il vostro trasferimento soddisfi gli standard di sostanziale equivalenza richiesti dal diritto dell'Unione.

100. A seconda di quali misure contrattuali sono già incluse nello strumento di trasferimento di cui all'articolo 46 del RGPD su cui si fa affidamento, possono essere utili anche misure contrattuali aggiuntive per consentire agli esportatori di dati con sede nel SEE di venire a conoscenza di nuovi sviluppi che incidono sulla protezione dei dati trasferiti verso paesi terzi.

101. Come detto, le misure contrattuali non potranno escludere l'applicazione della legislazione di un paese terzo che non soddisfa lo standard delle garanzie essenziali europee dell'EDPB nei casi in cui tale legislazione obbliga gli importatori a ottemperare agli ordini ricevuti dalle autorità pubbliche di comunicare i dati[92].

102. Alcuni esempi di queste possibili misure contrattuali sono elencati qui di seguito e classificati in base alla loro natura.

PREVEDERE L'OBBLIGO CONTRATTUALE DI UTILIZZARE MISURE TECNICHE SPECIFICHE

103. A seconda delle circostanze specifiche dei trasferimenti (ivi compresa l'applicazione concreta della legislazione del paese terzo), potrebbe essere necessario prevedere contrattualmente l'obbligo di attuare misure tecniche specifiche affinché i trasferimenti abbiano luogo (vedi sopra le misure tecniche suggerite).

104. Condizioni di efficacia:

- Questa clausola potrebbe essere efficace nelle situazioni in cui l'esportatore abbia individuato la necessità di misure tecniche. Dovrebbe quindi essere formulata giuridicamente in modo da garantire che anche l'importatore si impegni a mettere in atto le misure tecniche necessarie, se del caso.

OBBLIGHI DI TRASPARENZA

105. L'esportatore potrebbe aggiungere al contratto allegati contenenti informazioni che l'importatore avrà fornito prima della conclusione del contratto, con la massima diligenza possibile, in merito all'accesso ai dati da parte delle autorità pubbliche nel paese di destinazione, anche nel campo dell'intelligence, a condizione che la legislazione sia conforme alle garanzie essenziali europee dell'EDPB. Ciò potrebbe aiutare l'esportatore di dati a rispettare l'obbligo di documentare la valutazione del livello di protezione nel paese terzo. Così facendo si darebbe inoltre evidenza all'obbligo dell'importatore di assistere l'esportatore nella sua valutazione assumendosi la responsabilità di fornire, in tale contesto, informazioni che siano oggettive, pertinenti, attendibili, verificabili e disponibili al pubblico o altrimenti accessibili.

106. L'importatore potrebbe, ad esempio, essere obbligato a:

(1) elencare le leggi e i regolamenti del paese di destinazione applicabili all'importatore o ai suoi eventuali (sub)responsabili del trattamento che consentirebbero alle autorità pubbliche di accedere ai dati personali oggetto del trasferimento, in particolare nei settori dell'intelligence, delle attività giudiziarie e di polizia, del controllo amministrativo e regolamentare applicabile ai dati trasferiti;

(2) in assenza di norme che disciplinano l'accesso ai dati da parte delle autorità pubbliche, fornire informazioni e statistiche basate sull'esperienza dell'importatore o su relazioni provenienti da varie fonti (ad esempio partner commerciali, fonti pubbliche, giurisprudenza nazionale e decisioni degli organi di controllo) rispetto all'accesso da parte delle autorità pubbliche ai dati personali in situazioni assimilabili al trasferimento in questione (ad esempio nel settore normativo specifico; con riguardo alla categoria cui appartiene l'importatore di dati; ecc.);

(3) indicare quali misure sono adottate per impedire l'accesso ai dati trasferiti (se del caso);

(4) fornire informazioni sufficientemente dettagliate su tutte le richieste di accesso ai dati personali da parte delle autorità pubbliche ricevute dall'importatore in un determinato periodo di tempo[93], in particolare nei settori di cui al punto 1), fra cui informazioni sulle richieste ricevute, sui dati richiesti, sull'organismo richiedente, sulla base giuridica ai fini della comunicazione e sulla misura in cui l'importatore ha ottemperato alla richiesta di dati[94];

specificare se e in quale misura all'importatore sia proibito per legge fornire le informazioni di cui ai punti da 1) a 5).

107. Tali informazioni potrebbero essere fornite mediante questionari strutturati che l'importatore dovrebbe compilare e firmare e che sarebbero integrati dall'obbligo contrattuale dell'importatore di segnalare entro un intervallo determinato eventuali modifiche a tali informazioni, come è prassi corrente per i processi di *due diligence*.

108. Condizioni di efficacia:

- L'importatore deve essere in grado di fornire all'esportatore questo tipo di informazioni al meglio delle proprie conoscenze e dopo essersi adoperato al massimo per ottenerle.
- Questo obbligo imposto all'importatore è un mezzo per garantire che l'esportatore diventi e rimanga consapevole dei rischi connessi al trasferimento dei dati verso un paese terzo. Ciò consentirà quindi all'esportatore di desistere dalla conclusione del contratto o, se le informazioni cambiano successivamente alla stipula, di adempiere all'obbligo di sospendere il trasferimento e/o risolvere il contratto se la legge del paese terzo, le garanzie previste dallo strumento di trasferimento di cui all'articolo 46 del RGPD utilizzato e le eventuali garanzie supplementari da esso adottate non possono più garantire un livello di protezione sostanzialmente equivalente a quello del SEE. Il rispetto di tale obbligo non può tuttavia giustificare la comunicazione dei dati personali da parte dell'importatore, né far presumere che non vi saranno ulteriori richieste di accesso.

***

109. L'esportatore potrebbe anche aggiungere clausole in base alle quali l'importatore certifica che 1) non ha creato intenzionalmente backdoor o programmi simili che potrebbero essere utilizzati per accedere al sistema e/o ai dati personali, 2) non ha creato o modificato intenzionalmente i suoi processi commerciali in modo da facilitare l'accesso ai dati personali o ai sistemi, e 3) il diritto nazionale o la politica governativa non impongono all'importatore di creare o mantenere backdoor o di agevolare l'accesso ai dati personali o ai sistemi, o di essere in possesso o consegnare la chiave di cifratura[95].

110. Condizioni di efficacia:

- L'esistenza di una legislazione o di politiche governative che impediscono agli importatori di comunicare le informazioni in questione può rendere inefficace tale clausola. L'importatore non sarà quindi in grado di stipulare il contratto o dovrà comunicare all'esportatore la sua incapacità di continuare a rispettare gli impegni contrattuali.
- Il contratto deve includere sanzioni e/o la possibilità per l'esportatore di risolvere il contratto con breve preavviso nei casi in cui l'importatore non riveli l'esistenza di una backdoor o di un programma simile o di processi aziendali manipolati o l'obbligo di attuare uno di essi o non informi tempestivamente l'esportatore non appena venga a conoscenza della loro esistenza.
- Nel caso in cui l'importatore di dati abbia comunicato dati personali trasferiti violando gli impegni previsti dallo strumento di trasferimento, il contratto potrebbe altresì prevedere un risarcimento da parte dell'importatore di dati a beneficio dell'interessato per i danni materiali e immateriali subiti.

***

111. L'esportatore potrebbe rafforzare il suo potere di effettuare verifiche[96] o ispezioni delle strutture di trattamento dei dati dell'importatore, in loco e/o da remoto, per verificare se i dati siano stati comunicati alle autorità pubbliche e a quali condizioni (accesso non oltre quanto necessario e proporzionato in una società democratica), ad esempio prevedendo un breve preavviso e meccanismi che garantiscano il rapido intervento degli organismi ispettivi e rafforzino l'autonomia dell'esportatore nella scelta degli stessi.

112. Condizioni di efficacia:

- Per essere pienamente efficace, l'ambito della verifica deve includere giuridicamente e tecnicamente qualsiasi trattamento dei dati personali trasmessi nel paese terzo che sia svolto da parte dei (sub)responsabili del trattamento operanti per l'importatore.
- I registri di accesso e altri registri simili dovrebbero essere a prova di manomissione (per esempio dovrebbero essere resi inalterabili per mezzo di tecniche di cifratura conformi allo stato dell'arte, come l'hashing, ed essere inoltre trasmessi sistematicamente e periodicamente all'esportatore) in modo che i soggetti incaricati delle verifiche possano trovare evidenze di eventuali comunicazioni. I registri di accesso e altri registri simili dovrebbero inoltre distinguere tra gli accessi dovuti a regolari operazioni commerciali e gli accessi dovuti a ordini o richieste di accesso.

***

113. Qualora a seguito della valutazione iniziale del diritto e delle prassi del paese terzo dell'importatore si sia ritenuta la sussistenza di un livello di protezione sostanzialmente equivalente a quello previsto nell'UE per i dati trasferiti dall'esportatore, quest'ultimo potrebbe comunque rafforzare l'obbligo dell'importatore dei dati di informare tempestivamente l'esportatore, ove la situazione si modifichi, dell'impossibilità di rispettare gli impegni contrattuali e di conseguenza lo standard richiesto di «sostanziale equivalenza» del livello di protezione dei dati[97].

114. Tale impossibilità può derivare da cambiamenti nella legislazione o nelle prassi del paese terzo[98]. Le clausole potrebbero stabilire termini e procedure specifici e rigorosi per la rapida sospensione del trasferimento dei dati e/o la risoluzione del contratto e la restituzione o la cancellazione dei dati ricevuti da parte dell'importatore. Il monitoraggio delle richieste ricevute, della loro portata e dell'efficacia delle misure adottate per opporvisi dovrebbero fornire all'esportatore indicazioni sufficienti per adempiere all'obbligo di sospendere o terminare il trasferimento e/o risolvere il contratto.

115. Condizioni di efficacia:

- La notifica deve avvenire prima di consentire l'accesso ai dati. In caso contrario, al momento in cui l'esportatore riceve la notifica, i diritti della persona potrebbero essere già stati violati se la richiesta si basa su norme di tale paese terzo che eccedono quanto è consentito in base al livello di protezione dei dati previsto dal diritto dell'Unione. La notifica può comunque servi-

re a prevenire future violazioni e a consentire all'esportatore di adempiere all'obbligo di sospendere il trasferimento dei dati personali verso il paese terzo e/o di rescindere il contratto.

- L'importatore di dati deve monitorare qualsiasi sviluppo giuridico o politico che potrebbe comportare l'incapacità di adempiere agli obblighi rispettivamente incombenti e informare tempestivamente l'esportatore di tali sviluppi, se possibile prima della loro realizzazione, in modo da consentire all'esportatore di recuperare i dati.
- Le clausole dovrebbero prevedere un meccanismo rapido in base al quale l'esportatore di dati autorizza l'importatore di dati a mettere in sicurezza o a restituire prontamente i dati all'esportatore o, se ciò non è fattibile, a cancellare o cifrare in modo sicuro i dati senza necessariamente attendere le istruzioni dell'esportatore, se viene raggiunta una soglia specifica[99] da concordare tra l'esportatore e l'importatore di dati. L'importatore dovrebbe attuare questo meccanismo fin dall'inizio del trasferimento dei dati e testarlo regolarmente per garantire che possa essere applicato con un breve preavviso.
- Altre clausole potrebbero consentire all'esportatore di controllare il rispetto di tali obblighi da parte dell'importatore attraverso verifiche, ispezioni e altre misure di verifica e di farle rispettare attraverso sanzioni per l'importatore e/o il potere dell'esportatore di sospendere il trasferimento e/o di rescindere immediatamente il contratto.

***

116. Nella misura consentita dalla legislazione nazionale del paese terzo, il contratto potrebbe rafforzare gli obblighi di trasparenza dell'importatore prevedendo il ricorso al cosiddetto «Warrant Canary», per cui l'importatore si impegna a pubblicare regolarmente (ad esempio, almeno ogni 24 ore) un messaggio firmato in forma cifrata con cui informa l'esportatore che fino a una certa data e ora non ha ricevuto alcun ordine di rivelare dati personali o simili. Il mancato aggiornamento di questa comunicazione indicherà all'esportatore che l'importatore potrebbe aver ricevuto un ordine in tal senso.

117. Condizioni di efficacia:

- Le norme del paese terzo devono consentire all'importatore di dati di emettere questa forma di notifica passiva all'esportatore.
- L'esportatore di dati deve controllare automaticamente le comunicazioni warrant canary.
- L'importatore di dati deve garantire la conservazione sicura della sua chiave privata per la firma del warrant canary e che la legislazione del paese terzo non possa obbligarlo a emettere falsi warrant canary. A tal fine, potrebbe essere utile prevedere l'apposizione di più firme da parte di persone diverse e/o l'emissione del warrant canary da parte di una persona non soggetta alla giurisdizione del paese terzo.

OBBLIGHI DI INTRAPRENDERE AZIONI SPECIFICHE

118. L'importatore potrebbe impegnarsi a verificare, in base al diritto del paese di destinazione, la legalità di eventuali ordini di comunicazione dei dati, in particolare se essi eccedano i poteri riconosciuti all'autorità pubblica richiedente, e a contestare tali ordini se, dopo un'attenta valutazione, conclude che vi sono motivi per farlo in base al diritto del paese di destinazione. Nel contestare un ordine, l'importatore di dati dovrebbe chiedere misure provvisorie atte a sospendere gli effetti dello stesso fino a quando l'autorità giudiziaria non si sarà pronunciata nel merito. L'importatore avrà l'obbligo di non comunicare i dati personali richiesti fino a quando non sia tenuto a farlo in base alle norme applicabili. L'importatore si impegnerà inoltre a fornire la quantità minima consentita di informazioni in risposta all'ordine, sulla base di un'interpretazione ragionevole dello stesso.

119. Condizioni di efficacia:

- L'ordinamento giuridico del paese terzo deve offrire vie legali efficaci per contestare gli ordini di comunicazione dei dati.
- Questa clausola offrirà sempre una protezione aggiuntiva molto limitata, poiché un ordine di comunicare i dati può essere legittimo secondo l'ordinamento giuridico del paese terzo, ma tale ordinamento giuridico potrebbe non soddisfare gli standard dell'Unione. Questa misura contrattuale dovrà necessariamente essere integrata da altre misure supplementari.
- Le contestazioni degli ordini devono avere un effetto sospensivo ai sensi del diritto del paese terzo. In caso contrario, le autorità pubbliche avrebbero comunque accesso ai dati delle persone fisiche e qualsiasi azione conseguente a favore delle stesse avrebbe l'effetto limitato di consentire loro di chiedere il risarcimento dei danni per le conseguenze negative derivanti dalla comunicazione dei dati.
- L'importatore dovrà essere in grado di documentare e dimostrare all'esportatore le azioni che ha intrapreso, adoperandosi al massimo delle proprie possibilità, per adempiere a questo impegno.

***

120. Nella situazione sopra descritta, l'importatore potrebbe impegnarsi a informare l'autorità pubblica richiedente dell'incompatibilità dell'ordine rispetto alle garanzie previste dallo strumento di trasferimento di cui all'articolo 46 del RGPD[100] e del conseguente conflitto di obblighi per l'importatore. L'importatore informerebbe contemporaneamente e al più presto possibile l'esportatore e/o l'autorità di controllo competente del SEE, nella misura del possibile ai sensi dell'ordinamento giuridico del paese terzo.

121. Condizioni di efficacia:

- Le informazioni sulla protezione conferita dal diritto dell'Unione e sul conflitto di obblighi dovrebbero avere un qualche effetto giuridico nell'ordinamento del paese terzo per potenziare la protezione dei dati, come ad esem-

pio provocare un riesame in sede giudiziaria o amministrativa dell'ordine o della richiesta di accesso, rendere necessario un mandato giudiziario e/o imporre una sospensione temporanea dell'ordine.

- L'ordinamento giuridico del paese non deve impedire all'importatore di informare l'esportatore o almeno l'autorità di controllo competente del SEE dell'ordine o della richiesta di accesso ricevuta.
- L'importatore dovrà essere in grado di documentare e dimostrare all'esportatore le azioni che ha intrapreso, adoperandosi al massimo delle proprie possibilità, per adempiere a questo impegno.

CONSENTIRE AGLI INTERESSATI DI ESERCITARE I LORO DIRITTI

122. Il contratto potrebbe consentire l'accesso ai dati personali trasmessi in chiaro nel corso della normale attività commerciale (anche in contesti di supporto) solo previo accordo espresso o implicito dell'esportatore e/o dell'interessato, con riguardo a uno specifico accesso ai dati.

123. Condizioni di efficacia:

- Questa clausola potrebbe essere efficace in quelle situazioni in cui gli importatori ricevono richieste di cooperazione su base volontaria da parte delle autorità pubbliche, in contrapposizione, ad esempio, all'accesso ai dati da parte delle autorità pubbliche effettuato all'insaputa dell'importatore o contro la sua volontà.
- In alcune situazioni l'interessato potrebbe non essere in grado di opporsi all'accesso o di prestare un consenso che soddisfi tutte le condizioni stabilite dal diritto dell'Unione (libero, specifico, informato e inequivocabile) (ad esempio nel caso di lavoratori dipendenti)[101].
- Eventuali normative o prassi nazionali che obblighino l'importatore a non divulgare l'ordine di accesso possono rendere inefficace questa clausola, a meno di rafforzarla prevedendo tecnicamente la necessità di un intervento dell'esportatore o dell'interessato affinché i dati in chiaro siano resi accessibili. Tali misure tecniche volte a limitare l'accesso possono essere previste in particolare se l'accesso è consentito solo in casi specifici relativi ad attività di supporto o di servizio, ma i dati in quanto tali sono conservati nel SEE.

***

124. Il contratto potrebbe obbligare l'importatore e/o l'esportatore a comunicare tempestivamente all'interessato la richiesta o l'ordine ricevuto dalle autorità pubbliche del paese terzo, o l'impossibilità da parte dell'importatore di rispettare gli impegni contrattuali, così da consentire all'interessato di chiedere informazioni e di esperire un mezzo di ricorso effettivo (ad esempio presentando un reclamo all'autorità di controllo competente e/o all'autorità giudiziaria e dimostrando la propria legittimazione attiva dinanzi alle autorità giudiziarie del paese terzo), con la possibilità di prevedere un risarcimento da parte dell'importatore di dati per tutti i danni materiali

e immateriali subiti dell'interessato a causa della comunicazione dei dati personali trasferiti per mezzo dello strumento di trasferimento prescelto in violazione degli impegni da quest'ultimo previsti.

125. Condizioni di efficacia:

- Questa comunicazione potrebbe allertare l'interessato rispetto a potenziali accessi ai suoi dati da parte di autorità pubbliche di paesi terzi. Potrebbe così consentire all'interessato di chiedere informazioni aggiuntive agli esportatori e di presentare un reclamo all'autorità di controllo competente. Questa clausola potrebbe anche contribuire a risolvere alcune delle difficoltà che un interessato può incontrare nel dimostrare la propria legittimazione attiva (locus standi) dinanzi alle autorità giudiziarie di paesi terzi per contestare l'accesso ai propri dati da parte delle autorità pubbliche.
- Le normative e le politiche nazionali possono vietare questa comunicazione all'interessato. L'esportatore e l'importatore potrebbero tuttavia impegnarsi a informare l'interessato non appena le restrizioni alla suddetta comunicazione siano revocate e a compiere ogni sforzo possibile per ottenere la deroga al divieto di comunicazione. Come minimo, l'esportatore o l'autorità di controllo competente potrebbero comunicare all'interessato la sospensione o la cessazione del trasferimento dei suoi dati personali a causa dell'impossibilità per l'importatore di adempiere ai suoi impegni contrattuali a seguito della ricezione di una richiesta di accesso.

***

126. Il contratto potrebbe impegnare l'esportatore e l'importatore ad assistere l'interessato nell'esercizio dei suoi diritti nel paese terzo mediante appositi meccanismi di ricorso e consulenza legale.

127. Condizioni di efficacia:

- Alcune normative nazionali potrebbero non consentire all'importatore di dati di prestare questo tipo di assistenza direttamente agli interessati, benché possano permettergli di procurare tale assistenza a loro beneficio.
- Le normative e le prassi nazionali possono imporre condizioni tali da compromettere l'efficacia degli appositi meccanismi di ricorso previsti.
- La consulenza legale potrebbe essere utile per l'interessato, soprattutto considerando quanto complesso e costoso possa essere per lo stesso comprendere il sistema giuridico di un paese terzo ed esercitare azioni legali dall'estero, potenzialmente in una lingua straniera. Tuttavia, questa clausola offrirà sempre una protezione aggiuntiva limitata, poiché la prestazione di assistenza e consulenza legale agli interessati non può di per sé porre rimedio all'incapacità dell'ordinamento giuridico di un paese terzo di fornire un livello di protezione sostanzialmente equivalente a quello garantito all'interno del SEE. Questa misura contrattuale dovrà necessariamente essere integrata da altre misure supplementari.
- Questa misura supplementare sarebbe efficace solo a condizione che il diritto del paese terzo preveda mezzi di ricorso dinanzi alle autorità giudizia-

rie nazionali, o che esista un meccanismo di ricorso apposito, anche contro le misure di sorveglianza.

2.3 MISURE ORGANIZZATIVE

128. Ulteriori misure organizzative possono consistere in politiche interne, metodi organizzativi e standard che i titolari e i responsabili del trattamento potrebbero applicare a se stessi e imporre agli importatori di dati in paesi terzi. Esse possono contribuire a garantire la coerenza della protezione dei dati personali durante l'intero ciclo del trattamento. Le misure organizzative possono anche migliorare la consapevolezza degli esportatori rispetto ai rischi e ai tentativi di accedere ai dati nei paesi terzi e la loro capacità di reagire in tali frangenti. La selezione e l'attuazione di una o più di queste misure non garantirà necessariamente e sistematicamente che il vostro trasferimento soddisfi gli standard di sostanziale equivalenza richiesti dal diritto dell'Unione. A seconda delle circostanze specifiche del trasferimento e della valutazione effettuata sulla legislazione del paese terzo, sono necessarie misure organizzative per integrare le misure contrattuali e/o tecniche, al fine di garantire un livello di protezione dei dati personali sostanzialmente equivalente a quello garantito all'interno del SEE.

129. La valutazione delle misure più idonee deve essere effettuata caso per caso, tenendo presente che i titolari e i responsabili del trattamento devono rispettare il principio di responsabilizzazione. Di seguito, l'EDPB elenca alcuni esempi di misure organizzative che gli esportatori possono attuare. L'elenco non è esaustivo e possono essere appropriate anche altre misure.

POLITICHE INTERNE PER LA GOVERNANCE DEI TRASFERIMENTI, IN PARTICOLARE NEI GRUPPI DI IMPRESE

130. Adozione di adeguate politiche interne con una chiara attribuzione delle responsabilità per il trasferimento dei dati, canali di segnalazione e procedure operative standard in caso di richieste formali o informali di accesso ai dati da parte di autorità pubbliche. Soprattutto in caso di trasferimenti tra gruppi di imprese, tali politiche possono includere, tra l'altro, la nomina di un team specifico, composto da esperti in materia di informatica e legislazione in materia di protezione dei dati e privacy, per gestire le richieste che riguardano dati personali trasferiti dal SEE; la comunicazione alla direzione legale e aziendale e all'esportatore di dati al ricevimento di tali richieste; i passaggi procedurali per contestare richieste sproporzionate o illegali e la fornitura di informazioni trasparenti agli interessati.

131. Sviluppo di procedure di formazione specifiche per il personale incaricato di gestire le richieste di accesso ai dati personali da parte delle autorità pubbliche, che dovrebbero essere periodicamente aggiornate per riflettere i nuovi sviluppi legislativi e giurisprudenziali nel paese terzo e nel SEE. Le procedure di formazione dovrebbero includere i requisiti del diritto dell'U-

nione in materia di accesso ai dati personali da parte delle autorità pubbliche, in particolare come previsto dall'articolo 52, paragrafo 1, della Carta dei diritti fondamentali. Il personale dovrebbe essere sensibilizzato in particolare mediante la valutazione di esempi pratici di richieste di accesso ai dati da parte delle autorità pubbliche e applicando a tali esempi pratici la norma di cui all'articolo 52, paragrafo 1, della Carta dei diritti fondamentali. Tale formazione dovrebbe tener conto della situazione particolare dell'importatore di dati, ad esempio della legislazione e dei regolamenti del paese terzo a cui l'importatore di dati è soggetto, e dovrebbe essere elaborata, ove possibile, in collaborazione con l'esportatore di dati.

132. Condizioni di efficacia:

- Queste politiche possono essere previste solo nei casi in cui la richiesta delle autorità pubbliche del paese terzo è compatibile con il diritto dell'Unione[102]. Quando la richiesta è incompatibile, tali politiche non sarebbero sufficienti a garantire un livello equivalente di protezione dei dati personali e, come già indicato, i trasferimenti devono essere interrotti o devono essere messe in atto misure supplementari adeguate per evitare l'accesso.

MISURE A FINI DI TRASPARENZA E RESPONSABILIZZAZIONE

133. Documentare e registrare le richieste di accesso ricevute dalle autorità pubbliche e la risposta fornita, insieme alla motivazione giuridica e ai soggetti coinvolti (ad esempio se l'esportatore è stato informato e quale sia stata la sua risposta, la valutazione del team incaricato di trattare tali richieste, ecc.). Tali registrazioni dovrebbero essere messe a disposizione dell'esportatore, che dovrebbe a sua volta fornirle agli interessati.

134. Condizioni di efficacia:

- La legislazione nazionale del paese terzo può vietare la divulgazione delle richieste o delle informazioni di merito e quindi rendere inefficace questa prassi. L'importatore di dati dovrebbe informare l'esportatore dell'impossibilità di fornire tali documenti e registrazioni, offrendogli così la possibilità di sospendere i trasferimenti se ciò comportasse la mancanza di un livello di protezione adeguato.

***

135. La pubblicazione regolare di relazioni sulla trasparenza o di sintesi riguardanti le richieste governative di accesso ai dati e la tipologia delle risposte fornite, nella misura in cui tale pubblicazione è consentita dalla legislazione nazionale.

136. Condizioni di efficacia:

- Le informazioni fornite devono essere pertinenti, chiare e il più possibile dettagliate. La legislazione nazionale del paese terzo può impedire la divulgazione di informazioni dettagliate. In questi casi, l'importatore di dati

dovrebbe adoperarsi al meglio per pubblicare informazioni statistiche o informazioni aggregate di tipo analogo.

METODI DI ORGANIZZAZIONE E MISURE DI MINIMIZZAZIONE DEI DATI

137. Anche i requisiti organizzativi già esistenti in base al principio di responsabilizzazione, quali l'adozione di politiche di accesso ai dati e di riservatezza rigorose e granulari, e migliori pratiche basate sulla rigorosa applicazione del principio di necessità ("need to know"), monitorate regolarmente e attuate- con l'aiuto di misure disciplinari, possono risultare utili in un contesto di trasferimento dei dati. A questo proposito si dovrebbe prendere in considerazione la minimizzazione dei dati, al fine di limitare l'esposizione dei dati personali ad accessi non autorizzati. Ad esempio, in alcuni casi potrebbe non essere necessario trasferire determinati dati (si veda il caso di un accesso remoto ai dati SEE, come nelle attività di supporto, quando è previsto un accesso limitato anziché completo; oppure quando la fornitura di un servizio richiede solo il trasferimento di un set di dati limitato e non di un'intera banca dati).

138. Condizioni di efficacia:

- Dovrebbero essere previste verifiche regolari e misure disciplinari importanti per monitorare e far rispettare le misure di minimizzazione dei dati anche nel contesto del trasferimento.
- L'esportatore di dati effettua una valutazione dei dati personali in suo possesso prima che il trasferimento abbia luogo, al fine di individuare i set di dati che non sono necessari ai fini del trasferimento e che quindi non saranno condivisi con l'importatore di dati.
- Le misure di minimizzazione dei dati devono essere accompagnate da misure tecniche atte a garantire che i dati non siano soggetti ad accesso non autorizzato. Ad esempio, l'applicazione di meccanismi di calcolo multilaterali (multi-party computation) sicuri e la disseminazione di set di dati cifrati tra più soggetti fiduciari può impedire, fin dalla progettazione, che un eventuale accesso unilaterale comporti la divulgazione di dati identificabili.

***

139. Sviluppo di migliori prassi per coinvolgere in modo appropriato e tempestivo e informare il responsabile della protezione dei dati, se esistente, e i servizi legali e di revisione interna su questioni relative ai trasferimenti internazionali di dati personali.

140. Condizioni di efficacia:

- Il responsabile della protezione dei dati, se esistente, e il team legale e di revisione interna ricevono tutte le informazioni pertinenti prima del trasferimento e sono consultati sulla necessità del trasferimento e sulle eventuali garanzie supplementari.

- Le informazioni pertinenti devono comprendere, ad esempio, la valutazione della necessità del trasferimento dei dati personali specifici, una panoramica delle normative del paese terzo applicabili e le garanzie che l'importatore si è impegnato ad attuare.

ADOZIONE DI STANDARD E MIGLIORI PRASSI

141. Adozione di politiche rigorose in materia di sicurezza e riservatezza dei dati, basate sulla certificazione UE o su codici di condotta o su standard internazionali (ad esempio norme ISO) e sulle migliori prassi (ad esempio ENISA), nel rispetto dello stato dell'arte, in funzione del rischio delle categorie di dati trattati.

ALTRE

142. Adozione e revisione periodica delle politiche interne per valutare l'adeguatezza delle misure supplementari attuate e individuare e attuare soluzioni aggiuntive o alternative, se necessario, per garantire il mantenimento di un livello di protezione dei dati personali trasferiti sostanzialmente equivalente a quello garantito all'interno del SEE.

***

143. L'impegno dell'importatore di dati a non effettuare trasferimenti successivi dei dati personali all'interno dello stesso paese o verso altri paesi terzi, o a sospendere i trasferimenti in corso, qualora non possa essere garantito nel paese terzo un livello di protezione dei dati personali sostanzialmente equivalente a quello garantito all'interno del SEE[103].

ALLEGATO 3: POSSIBILI FONTI DI INFORMAZIONI PER VALUTARE UN PAESE TERZO

144. Il vostro importatore di dati dovrebbe essere in grado di fornirvi le fonti e le informazioni pertinenti relative al paese terzo in cui è stabilito, ivi comprese le normative e le prassi applicabili all'importatore stesso e ai dati trasferiti. Voi e l'importatore potete fare riferimento a varie fonti di informazione, come quelle elencate di seguito in modo non esaustivo e in ordine di preferenza:

- giurisprudenza della Corte di giustizia dell'Unione europea (CGUE) e della Corte europea dei diritti dell'uomo (Corte CEDU)[104], come indicato nelle raccomandazioni relative alle garanzie essenziali europee[105];
- decisioni di adeguatezza nel paese di destinazione se il trasferimento si basa su una base giuridica diversa[106];
- risoluzioni e relazioni di organizzazioni intergovernative, quali il Consiglio d'Europa[107], altri organismi regionali[108] e organi e agenzie dell'ONU [ad esempio il Consiglio dei diritti umani delle Nazioni Unite[109] o il Comitato dei diritti umani[110]];
- relazioni e analisi a cura di reti di regolamentazione competenti come la Global Privacy Assembly (GPA)[111];
- giurisprudenza nazionale o decisioni adottate da autorità giudiziarie o amministrative indipendenti competenti in materia di privacy e di protezione dei dati di paesi terzi;
- relazioni pubblicate da organi parlamentari o di vigilanza indipendenti;
- relazioni pubblicate da soggetti attivi nello stesso settore dell'importatore basate sull'esperienza pratica relativa a casi pregressi di richieste di comunicazione da parte di autorità pubbliche, o all'assenza di tali richieste;
- warrant canary di altri soggetti che trattano dati nello stesso settore dell'importatore;
- relazioni prodotte o commissionate da camere di commercio, associazioni commerciali, professionali e di categoria, agenzie diplomatiche governative, commerciali e di investimento dell'esportatore o di altri paesi terzi che esportano nel paese terzo verso cui viene effettuato il trasferimento;
- relazioni di istituzioni accademiche e organizzazioni della società civile (ad esempio ONG);
- relazioni di fornitori privati di business intelligence in materia di rischi finanziari, normativi e reputazionali per le aziende;
- warrant canary dell'importatore stesso[112];
- relazioni sulla trasparenza, a condizione che menzionino espressamente il fatto che non sono pervenute richieste di accesso. Le relazioni sulla trasparenza che si limitino a tacere sul punto non sarebbero sufficientemente probanti, poiché il più delle volte riferiscono delle richieste di accesso pervenute da autorità giudiziarie e di polizia e forniscono dati solo su questo aspetto, mentre tacciono in merito a richieste di accesso ricevute per scopi di sicurezza nazionale. Ciò non significa che non siano pervenute richieste

di accesso, ma piuttosto che queste informazioni non possono essere condivise[113].

- dichiarazioni interne o registri dell'importatore che indicano espressamente che non sono pervenute richieste di accesso per un periodo sufficientemente lungo, preferibilmente dichiarazioni e registri che impegnano la responsabilità dell'importatore e/o che sono prodotti da funzioni interne dotate di margini di autonomia quali revisori interni, responsabili della protezione dei dati, ecc.[114]

NOTE

[1] Nel presente documento, con «Stati membri» si fa riferimento agli «Stati membri del SEE».

[2] Sentenza della CGUE del 16 luglio 2020, Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems, [in appresso: C-311/18 (Schrems II)], seconda conclusione.

[3] C-311/18 (Schrems II), paragrafi 92 e 93.

[4] C-311/18 (Schrems II), paragrafi 132 e 133.

[5] C-311/18 (Schrems II), paragrafo 134.

[6] C-311/18 (Schrems II), paragrafo 135.

[7] Articolo 70, paragrafo 1, lettera e), del RGPD.

[8] Articolo 8, paragrafo 1, della Carta dei diritti fondamentali e articolo 16, paragrafo 1, TFUE, primo preambolo e articolo 1, paragrafo 2, del RGPD.

[9] Articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea. Art

[10] Considerando 4 del RGPD e C-507/17, Google LLC, succeduta alla Google Inc., contro Commission nationale de l'informatique et des libertés (CNIL), paragrafo 60.

[11] C-92/09 e C-93/02, Volker und Markus Schecke GbR contro Land Hessen, conclusioni dell'avvocato generale Sharpston, 17 giugno 2010, paragrafo 71.

[12] Articolo 5, paragrafo 2, e articolo 28, paragrafo 3, lettera h), del RGPD.

[13] Articolo 44 e considerando 101 del RGPD, nonché articolo 47, paragrafo 2, lettera d), del RGPD

[14] Sentenza della Corte di giustizia dell'Unione europea del 6 ottobre 2015, *Maximillian Schrems contro Data Protection Commissioner* [di seguito «C-362 /14 (Schrems I)»], paragrafo 45.

[15] C-311/18 (Schrems II), paragrafi 92 e 93.

[16] C-311/18 (Schrems II), paragrafi 134, 135, 139, 140, 141 e 142.

[17] C-311/18 (Schrems II), paragrafo 134.

[18] Articolo 5, paragrafo 2, e articolo 28, paragrafo 3, lettera h), del RGPD.

[19] Perciò, per esempio, non si considerano esportatori di dati gli interessati che forniscono i propri dati personali per mezzo di un questionario online a un titolare del trattamento stabilito in un paese terzo.

[20] Cfr. Linee guida 3/2018 dell'EDPB sull'ambito di applicazione territoriale del RGPD (articolo 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en

[21] Linee guida 2/2020 dell'EDPB sull'articolo 46, paragrafo 2, lettera a), e sull'articolo 46, paragrafo 3, lettera b), del regolamento 2016/679 per i trasferimenti di dati personali tra autorità e organismi pubblici del SEE e di paesi non appartenenti al SEE; cfr. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_it

[22] Articolo 5, paragrafo 2, del RGPD e articolo 24, paragrafo 1, del RGPD.

[23] Si osservi che anche l'accesso remoto da parte di un'entità di un paese terzo a dati situati nel SEE è considerato un trasferimento.

[24] Cfr. articolo 30 del RGPD, in particolare il paragrafo 1, lettera e), e il paragrafo 2, lettera c). Inoltre, i vostri registri di trattamento devono contenere una descrizione delle attività di trattamento, comprese, tra l'altro, le categorie di persone interessate, le categorie di dati personali, le finalità del trattamento e informazioni specifiche sui trasferimenti di dati. Alcuni titolari del trattamento e responsabili del trattamento sono esonerati dall'obbligo di tenere i registri del trattamento (articolo 30, paragrafo 5, del RGPD). Per indicazioni su tale esenzione, si veda il documento di posizione del Gruppo di lavoro «Articolo 29» per la tutela dei dati sulle deroghe all'obbligo di tenere la documentazione delle attività di trattamento ai sensi dell'articolo 30, paragrafo 5, del RGPD (approvato dall'EDPB il 25 maggio 2018).

[25] In base alle regole di trasparenza del RGPD, dovete informare gli interessati dei trasferimenti di dati personali verso paesi terzi (articolo 13, paragrafo 1, lettera f), e articolo 14, paragrafo 1, lettera f), del RGPD). In particolare, dovete informarli dell'esistenza o dell'assenza di una decisione di adeguatezza da parte della Commissione europea o, nel caso di

trasferimenti di cui agli articoli 46 o 47 del RGPD, o al secondo comma dell'articolo 49, paragrafo 1, del RGPD, specificare le garanzie opportune o adeguate e i mezzi con cui ottenerne una copia ovvero il luogo dove sono state rese disponibili. Le informazioni fornite all'interessato devono essere corrette e aggiornate, soprattutto alla luce della giurisprudenza della Corte in materia di trasferimenti.

[26] Qualora il titolare del trattamento abbia rilasciato la previa autorizzazione scritta, specifica o generale, ai sensi dell'articolo 28, paragrafo 2, del RGPD.

[27] Articolo 5, paragrafo 1, lettera c), del RGPD.

[28] Cfr. la FAQ n. 11 «si tenga presente che anche fornire accesso ai dati da un paese terzo, ad esempio per finalità amministrative, costituisce un trasferimento», domande più frequenti dell'EDPB in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems, 23 luglio 2020.

[29] La Commissione europea ha il potere di determinare, sulla base dell'articolo 45 del RGPD, se un paese al di fuori dell'UE offre un livello adeguato di protezione dei dati. Analogamente, la Commissione europea ha il potere di stabilire se un'organizzazione internazionale offre un livello di protezione adeguato.

[30] Articolo 45, paragrafo 1, del RGPD.

[31] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[32] A condizione che voi e l'importatore di dati abbiate attuato misure volte a rispettare gli altri obblighi previsti dal RGPD; in caso contrario, attuate tali misure.

[33] La Commissione europea deve riesaminare periodicamente tutte le decisioni di adeguatezza e controllare se i paesi terzi che ne beneficiano continuano a garantire un livello di protezione adeguato (cfr. articolo 45, paragrafi 3 e 4, del RGPD). Inoltre, la CGUE può invalidare le decisioni di adeguatezza [cfr. le sentenze nelle cause C-362/14 (Schrems I) e C-311/18 (Schrems II)].

[34] C-311/18 (Schrems II), paragrafi 118-120. Le autorità di controllo non possono ignorare la decisione di adeguatezza e sospendere o vietare i trasferimenti di dati personali verso tali paesi citando solo l'inadeguatezza del livello di protezione. Esse possono esercitare il loro potere di sospendere o vietare i trasferimenti di dati personali verso tale paese terzo solo per altri motivi (ad esempio, misure di sicurezza insufficienti in violazione dell'articolo 32 del RGPD, o assenza di una valida base giuridica per il trattamento dei dati in quanto tale in violazione dell'articolo 6 del RGPD). Le autorità di controllo possono esaminare, in piena indipendenza, se il trasferimento di tali dati è conforme ai requisiti stabiliti dal RGPD e, se del caso, proporre un ricorso dinanzi al giudice nazionale affinché, in caso di dubbi sulla validità della decisione di adeguatezza della Commissione, sia presentata alla Corte di giustizia una domanda di pronuncia pregiudiziale ai fini dell'esame della validità.

[35] Causa C 362/14 (Schrems I).

[36] C-311/18 (Schrems II), paragrafi 130 e 133. Vedere anche la sottosezione 2.3 in appresso.

[37] Per ulteriori indicazioni in merito cfr. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_it.

[38] Articolo 44 del RGPD e C-311/18 (Schrems II), paragrafi 126, 137 e 148.

[39] C-311/18 (Schrems II), paragrafi 105 e seconda conclusione.

[40] Cfr. C-311/18 (Schrems II), paragrafo 183 in combinato disposto con il paragrafo 184.

[41] Cfr. il paragrafo 126 della sentenza C-311/18 (Schrems II), in cui la Corte allude espressamente al «diritto e [a]lle prassi vigenti nel paese terzo interessato» e richiede di «[...] garantire, in pratica, la protezione effettiva dei dati personali trasferiti nel paese terzo interessato» (sottolineatura aggiunta), e il paragrafo 158.

[42] Un trasferimento di dati personali è un'operazione di trattamento (articolo 4, paragrafo 2, RGPD). Se desiderate trasferire dati sensibili contemplati dall'ambito di applicazione degli articoli 9 e 10 del RGPD, potete effettuare un trasferimento solo se rientra nell'ambito di una delle deroghe e delle condizioni previste dagli articoli 9 e 10 del RGPD e dal diritto degli Stati membri dell'UE. Ai sensi dell'articolo 32 del RGPD, dovrete inoltre mettere in atto, con l'importatore che agisce in qualità di titolare del trattamento o responsabile del trattamento, misure tecniche e organizzative opportune per garantire un livello di sicurezza adeguato ai rischi per i diritti e le libertà degli interessati, costituiti da una potenziale violazione dei dati personali trasferiti (articolo 4, paragrafo 12, RGPD). Le categorie di dati trasferiti e la loro sensibilità saranno pertinenti per la valutazione del rischio e l'adeguatezza delle misure.

[43] Alcuni paesi terzi non consentono l'importazione di dati cifrati.

[44] Qualora il titolare del trattamento abbia rilasciato la previa autorizzazione scritta, specifica o

generale, ai sensi dell'articolo 28, paragrafo 2, del RGPD.

[45] Si vedano gli articoli 47 e 52 della Carta dei diritti fondamentali dell'Unione europea, l'articolo 23, paragrafo 1, del RGPD e le raccomandazioni 02/2020 dell'EDPB, del 10 novembre 2020, relative alle garanzie essenziali europee per le misure di sorveglianza, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-europeean-essential_en.

[46] Si vedano gli articoli 47 e 52 della Carta dei diritti fondamentali dell'Unione europea, l'articolo 23, paragrafo 1, del RGPD, C-311/18 (Schrems II), paragrafi 174 e 187, e le raccomandazioni 02/2020 dell'EDPB, del 10 novembre 2020, relative alle garanzie essenziali europee per le misure di sorveglianza.

[47] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020.

[48] E quindi non in contrasto con gli impegni assunti con lo strumento di trasferimento di cui all'articolo 46 del RGPD.

[49] C-311/18 (Schrems II), paragrafo 126.

[50] Per «legislazione problematica» si intende una legislazione che 1) impone obblighi sul destinatario del trasferimento di dati personali provenienti dall'Unione europea e/o influisce sui dati trasferiti in modo tale da poter pregiudicare la garanzia contrattuale, prevista dagli strumenti di riferimento, di un livello di protezione sostanzialmente equivalente e 2) non rispetta l'essenza dei diritti e delle libertà fondamentali riconosciuti dalla Carta dei diritti fondamentali dell'UE o va al di là di quanto necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi importanti riconosciuti anche dal diritto dell'Unione o degli Stati membri dell'UE, come quelli di cui all'articolo 23, paragrafo 1, del RGPD.

[51] Potrebbe non essere chiaro se l'importatore e/o i dati trasferiti rientrino o meno nell'ambito di applicazione delle disposizioni formulate spesso in termini generali nella normativa nazionale in materia di sicurezza, quali ad esempio «fornitore di servizi di comunicazioni elettroniche» e «informazioni di intelligence esterna».

[52] Cfr. considerando 109 del RGPD e C-311/18 (Schrems II), paragrafo 132.

[53] Cfr. punti da 45 a 47.

[54] Le relazioni che redigerete dovranno includere informazioni esaustive sulla valutazione giuridica della legislazione e delle prassi, nonché della loro applicazione ai trasferimenti specifici, la procedura interna impiegata per eseguire la valutazione (ivi comprese informazioni sugli attori in essa coinvolti: per esempio studi legali, consulenti o servizi interni) e le date delle verifiche. Le relazioni dovrebbero essere approvate dal legale rappresentante dell'esportatore.

[55] L'avvenuta dimostrazione della non applicabilità della legislazione problematica, in concreto, ai dati trasferiti e all'importatore, anche tenendo conto dell'esperienza di altri soggetti che operano nello stesso settore e/o in relazione a dati personali trasferiti di natura analoga, non vi esenta dal prevedere le misure supplementari necessarie per proteggere i dati personali durante la loro trasmissione e il trattamento nel paese terzo di destinazione (per esempio la cifratura end-to-end dei dati; cfr. gli esempi di misure tecniche supplementari nell'allegato 2) se la vostra analisi della legislazione applicabile del paese terzo di destinazione indica che l'accesso ai dati potrebbe verificarsi, anche in assenza dell'intervento dell'importatore, in questa fase del trasferimento. È possibile che abbiate già previsto tali misure con l'importatore che agisce in qualità di titolare del trattamento o responsabile del trattamento, ai sensi dell'articolo 32 del RGPD.

[56] Cfr. l'allegato 3 per un elenco non esaustivo di fonti di informazioni che voi e l'importatore potreste utilizzare.

[57] L'esperienza potrebbe essere quella di altri soggetti a voi noti direttamente per via di trasferimenti precedenti dello stesso tipo da voi effettuati, o quella riferita nella giurisprudenza pertinente, in relazioni a cura di ONG, ecc. (cfr. allegato 3).

[58] Articolo 5, paragrafo 2, del RGPD.

[59] C-311/18 (Schrems II), paragrafi 134 e 135.

[60] Per esempio disposizioni dell'articolo 702 della FISA, norme procedurali della Foreign Intelligence Surveillance Court (FISC), decisioni e pareri declassificati della FISC; giurisprudenza dei tribunali statunitensi; relazioni e trascrizioni di udienze dell'Autorità per la tutela della vita privata e delle libertà civili (Privacy and Civil Liberties Oversight Board, PCLOB); relazioni a cura dell'Ispettorato generale - Dipartimento della Giustizia statunitense; relazioni del direttore dell'Ufficio per la tutela della vita privata e delle libertà civili dell'NSA; relazioni a cura del Servizio di ricerca del Congresso; relazioni a cura dell'American Civil Liberties Union Foundation (ACLU).

[61] C-311/18 (Schrems II), paragrafo 96.

[62] Considerando 109 del RGPD e C-311/18 (Schrems II), paragrafo 133.

[63] Per «legislazione problema-

tica» si intende una legislazione che 1) impone obblighi sul destinatario del trasferimento di dati personali provenienti dall'Unione europea e/o influisce sui dati trasferiti in modo tale da poter pregiudicare la garanzia contrattuale, prevista dagli strumenti di riferimento, di un livello di protezione sostanzialmente equivalente e 2) non rispetta l'essenza dei diritti e delle libertà fondamentali riconosciuti dalla Carta dei diritti fondamentali dell'UE o va al di là di quanto necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi importanti riconosciuti anche dal diritto dell'Unione o degli Stati membri dell'UE, come quelli di cui all'articolo 23, paragrafo 1, del RGPD.

[64] Qualora tale accesso vada al di là di quanto necessario e proporzionato in una società democratica; cfr. gli articoli 47 e 52 della Carta dei diritti fondamentali dell'Unione europea, l'articolo 23, paragrafo 1, del RGPD e le raccomandazioni 02/2020 dell'EDPB, del 10 novembre 2020, relative alle garanzie essenziali europee per le misure di sorveglianza, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-europeaan-essential_en.

[65] Cfr. nota 42.

[66] Il RGPD attribuisce obblighi distinti ai titolari del trattamento e ai responsabili del trattamento. I trasferimenti possono avvenire da titolare del trattamento a titolare del trattamento, tra co-titolari del trattamento, da titolare del trattamento a responsabile del trattamento e, previa autorizzazione del titolare del trattamento, da responsabile del trattamento a titolare del trattamento o da responsabile del trattamento a responsabile del trattamento.

[67] Cfr. nota 26.

[68] Qualora tale accesso vada al di là di quanto necessario e proporzionato in una società democratica; cfr. gli articoli 47 e 52 della Carta dei diritti fondamentali dell'Unione europea, l'articolo 23, paragrafo 1, del RGPD e le raccomandazioni 02/2020 dell'EDPB, del 10 novembre 2020, relative alle garanzie essenziali europee per le misure di sorveglianza, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-europeaan-essential_en.

[69] C-311/18 (Schrems II), paragrafo 135.

[70] Cfr. per esempio la clausola 12 nell'allegato alla decisione 87/2010 sulle clausole contrattuali tipo; cfr. la clausola di risoluzione (facoltativa) nell'allegato B della decisione 2004/915/CE sulle clausole contrattuali tipo.

[71] Il considerando 109 del RGPD recita: «La possibilità che il titolare del trattamento o il responsabile del trattamento utilizzi clausole tipo di protezione dei dati adottate dalla Commissione o da un'autorità di controllo non dovrebbe precludere ai titolari del trattamento o ai responsabili del trattamento la possibilità di includere tali clausole tipo in un contratto più ampio, anche in un contratto tra il responsabile del trattamento e un altro responsabile del trattamento, né di aggiungere altre clausole o garanzie supplementari, purché non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo adottate dalla Commissione o da un'autorità di controllo o ledano i diritti o le libertà fondamentali degli interessati.» Disposizioni simili sono previste negli insiemi di clausole contrattuali tipo adottate dalla Commissione europea ai sensi della direttiva 95/45/CE.

[72] Si veda, per analogia, il parere 17/2020 dell'EDPB sul progetto di clausole contrattuali tipo presentato dall'autorità di controllo slovena (articolo 28, paragrafo 8, del RGPD) in merito a clausole contrattuali tipo ai sensi dell'art. 28 già adottate che contengono una disposizione analoga («In aggiunta, il comitato ricorda che la possibilità di usufruire delle clausole contrattuali tipo adottate da un'autorità di controllo non impedisce alle parti di aggiungere altre clausole o salvaguardie supplementari, a condizione che esse non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo adottate né pregiudichino i diritti o le libertà fondamentali degli interessati. Inoltre, in caso di modifica alle clausole contrattuali tipo sulla protezione dei dati, non si riterrà più che le parti abbiano dato esecuzione alle clausole contrattuali tipo adottate»), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_en.pdf.

[73] CGUE, C-311/18 (Schrems II), paragrafo 132.

[74] Gruppo di lavoro Articolo 29 per la protezione dei dati, Documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa, da ultimo riveduto e approvato il 6 febbraio 2018, WP 256 rev.01; Gruppo di lavoro Articolo 29 per la protezione dei dati, Documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa per i responsabili del trattamento, versione emendata e adottata da ultimo il 6 febbraio 2018, WP 257 rev.01.

[75] CGUE, C-311/18 (Schrems II), paragrafo 132.

[76] C-311/18 (Schrems II), paragrafo 93.

[77] Articolo 5, paragrafo 2, e articolo 32, del RGPD.

[78] C-311/18 (Schrems II), paragrafo 135.

[79] Si vedano gli articoli 47 e 52 della Carta dei diritti fondamentali dell'Unione europea, l'articolo 23, paragrafo 1, del RGPD e le raccomandazioni 02/2020 dell'EDPB, del 10 novembre 2020, relative alle garanzie essenziali europee per le misure di sorveglianza.

[80] Al fine di valutare l'efficacia degli algoritmi di cifratura, la loro conformità allo stato dell'arte e la loro solidità nel tempo rispetto alla crittoanalisi, gli esportatori di dati possono basarsi sugli orientamenti tecnici pubblicati dalle autorità ufficiali di cibersicurezza dell'UE e dei suoi Stati membri. Cfr. per esempio la relazione dell'ENISA «What is "state of the art" in IT security? », 2019, https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security; gli orientamenti forniti dall'Ufficio federale per la sicurezza delle tecniche dell'informazione nelle sue linee guida tecniche della serie TR-02102 e «Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018» all'indirizzo https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

[81] La capacità di protezione degli algoritmi crittografici è soggetta a declino nel corso del tempo per la scoperta di nuove tecniche crittoanalitiche, la comparsa di nuovi paradigmi di calcolo come l'informatica quantistica e l'aumento generale della potenza di calcolo disponibile, a meno che gli algoritmi applicati non si dimostrino teoricamente sicuri per le informazioni. Questo problema vale in particolare per gli algoritmi delle chiavi pubbliche che sono di uso comune al momento della stesura del presente documento. Di conseguenza, l'esportatore di dati deve considerare che le autorità pubbliche potrebbero impegnarsi ad accedere a dati cifrati nelle circostanze descritte al paragrafo n. 80 e archiviarli finché le loro risorse non saranno sufficienti per decifrarli. La misura supplementare può essere ritenuta efficace solo se tale decifrazione e l'ulteriore trattamento successivo non configurano più, in tale momento, una violazione dei diritti degli interessati, ad esempio perché i dati non possono più essere utilizzati per la loro identificazione diretta o indiretta.

[82] Pubblicazione speciale del NIST 800-57, Raccomandazione per la gestione delle chiavi, https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final.

[83] In linea con l'articolo 4, paragrafo 5, del RGPD: «"pseudonimizzazione": il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile». I dati aggiuntivi possono essere costituiti da tavole in cui gli pseudonimi vengono giustapposti agli attributi identificativi che sostituiscono, chiavi crittografiche o altri parametri per la trasformazione degli attributi, oppure altri dati che permettano di attribuire i dati pseudonimizzati a persone fisiche identificate o identificabili.

[84] Articolo 4, paragrafo 1, del RGPD: «"dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

[85] Cfr. la nota 80 per alcuni riferimenti agli orientamenti tecnici pubblicati dalle autorità ufficiali di cibersicurezza dell'UE e dei suoi Stati membri.

[86] Si vedano gli articoli 47 e 52 della Carta dei diritti fondamentali dell'Unione europea, l'articolo 23, paragrafo 1, del RGPD e le raccomandazioni 02/2020 dell'EDPB, del 10 novembre 2020, relative alle garanzie essenziali europee per le misure di sorveglianza.

[87] Indipendentemente dal fatto che sia un titolare o un responsabile del trattamento in un paese terzo a ricevere od ottenere accesso ai dati personali trasferiti dal SEE.

[88] Si tratta di accordi aventi carattere privato e non saranno considerati accordi internazionali ai sensi del diritto internazionale pubblico. Di conseguenza, di norma non vincoleranno l'autorità pubblica del paese terzo, in quanto parte non contraente, quando sono conclusi con organismi privati di paesi terzi, come sottolineato dalla Corte nella sentenza C-311/18 (Schrems II), paragrafo 125.

[89] Ad esempio nell'ambito delle norme vincolanti d'impresa, che dovrebbero in ogni caso disciplinare alcune delle misure elencate di seguito.

[90] Cfr. sentenza C-311/18 (Schrems II), paragrafo 137, in cui la Corte ha riconosciuto che le clausole contrattuali tipo contengono «meccanismi efficaci che [consentono], in pratica, di garantire che sia rispettato il livello di protezione richiesto dal diritto dell'Unione e che i trasferimenti di dati personali, fondati su siffatte clausole, siano sospesi o vietati

in caso di violazione di tali clausole o di impossibilità di rispettarle»; cfr. anche paragrafo 148.

[91] C-311/18 (Schrems II), paragrafo 125.

[92] Sentenza della CGUE C-311 /18 (Schrems II), paragrafo 132.

[93] Tale lasso di tempo dovrebbe dipendere dal rischio per i diritti e le libertà degli interessati i cui dati sono oggetto del trasferimento in questione: ad esempio, l'ultimo anno prima del perfezionamento dello strumento di esportazione dei dati con l'esportatore di dati.

[94] Il rispetto di questo obbligo non equivale, in quanto tale, alla prestazione di un livello di protezione adeguato. Al tempo stesso, qualsiasi comunicazione impropria che sia effettivamente avvenuta porta alla necessità di attuare misure supplementari.

[95] Questa clausola è importante per garantire un adeguato livello di protezione dei dati personali trasferiti e dovrebbe essere richiesta in via routinaria.

[96] Si veda ad esempio la clausola 5, lettera f), della decisione 2010/87/UE relativa alle clausole contrattuali tipo tra titolari e responsabili del trattamento; le verifiche potrebbero essere effettuate anche nell'ambito di un codice di condotta o mediante certificazione.

[97] Clausola 5, lettera a) e lettera d), punto i) della decisione 2010/87/UE relativa alle clausole contrattuali tipo.

[98] Cfr. C-311/18 (Schrems II), paragrafo 139, in cui la Corte afferma che «se è vero che la stessa clausola 5, lettera d), i), consente al destinatario del trasferimento di dati personali, in presenza di legislazione che gliene faccia divieto, ad esempio norme di diritto penale miranti a tutelare il segreto delle indagini, di non comunicare al titolare del trattamento stabilito nell'Unione una richiesta giuridicamente vincolante presentata da autorità giudiziarie o di polizia ai fini della comunicazione di dati personali, egli è tuttavia tenuto, conformemente alla clausola 5, lettera a), dell'allegato della decisione CPT, ad informare il titolare del trattamento dell'impossibilità di conformarsi alle clausole tipo di protezione dei dati».

[99] Tale soglia dovrebbe garantire che gli interessati continuino a godere di un livello di protezione equivalente a quello garantito all'interno del SEE.

[100] Ad esempio, le clausole contrattuali tipo prevedono che il trattamento dei dati, compreso il loro trasferimento, sia stato e continui a essere effettuato in conformità alla «*legge applicabile in materia di protezione dei dati*». Tale legge è definita come «*la legislazione che tutela i diritti e le libertà fondamentali delle persone fisiche e, in particolare, il loro diritto al rispetto della vita privata in relazione al trattamento dei dati personali applicabile a un titolare del trattamento dei dati nello Stato membro in cui è stabilito l'esportatore di dati*». La CGUE conferma che le disposizioni del RGPD, lette alla luce della Carta dei diritti fondamentali dell'Unione, fanno parte di tale legislazione; cfr. CGUE C-311/18 (Schrems II), paragrafo 138.

[101] Articolo 4, paragrafo 11, del RGPD.

[102] Cfr. causa C 362/14 («Schrems I»), paragrafo 94; C-311/18 (Schrems II), paragrafi 168, 174, 175 e 176.

[103] C-311/18 (Schrems II), paragrafi 135 e 137.

[104] Si veda la scheda della giurisprudenza della Corte CEDU sulla sorveglianza di massa: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[105] Raccomandazioni 02/2020 dell'EDPB, del 10 novembre 2020, relative alle garanzie essenziali europee per le misure di sorveglianza, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[106] C-311/18 (Schrems II), paragrafo 141; cfr. decisioni di adeguatezza in https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[107] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[108] Cfr., ad esempio, i rapporti sui paesi della Commissione interamericana dei diritti dell'uomo (IACHR), https://www.oas.org/en/iachr/reports/country.asp.

[109] Cfr. https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx.

[110] Cfr. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5.

[111] Cfr. per esempio https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

[112] Cfr. le condizioni per tenere conto dell'esperienza pratica documentata dell'importatore rispetto a casi pregressi e pertinenti di richieste di accesso pervenute da autorità pubbliche nel paese terzo di cui al paragrafo 47.

[113] *Ibid.*

[114] *Ibid.*

Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza

Adottate il 10 novembre 2020

Indice

1 Introduzione

2. Ingerenze nei diritti fondamentali

3. Le garanzie essenziali europee
   Garanzia A - Il trattamento deve basarsi su regole chiare, precise e accessibili
   Garanzia B - Devono essere dimostrate la necessità e la proporzionalità rispetto agli obiettivi legittimi perseguiti
   Garanzia C - Meccanismo di controllo indipendente
   Garanzia D - La persona deve poter accedere a mezzi di ricorso efficaci

4. Osservazioni conclusive

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettera e), del regolamento 2016/679/UE del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in appresso: il «RGPD»)[1],

visto l'accordo SEE, in particolare l'allegato XI e il protocollo n. 37 dello stesso, modificati dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018[2],

visto l'articolo 12 e l'articolo 22 del regolamento interno,

visto il documento di lavoro del Gruppo "Articolo 29" sulla giustificazione delle ingerenze nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati mediante misure di sorveglianza nel contesto del trasferimento di dati personali (garanzie essenziali europee), WP237,

HA ADOTTATO LE SEGUENTI RACCOMANDAZIONI:

INTRODUZIONE

1. A seguito della sentenza Schrems I, le autorità competenti per la protezione dei dati personali dell'UE riunite nel gruppo "Articolo 29" hanno fatto riferimento alla giurisprudenza per individuare le garanzie essenziali europee che devono essere rispettate al fine di garantire che, in rapporto al trasferimento di dati personali, le ingerenze nei diritti al rispetto della vita privata e alla protezione dei dati personali mediante misure di sorveglianza non eccedano quanto è necessario e proporzionato in una società democratica.

2. L'EDPB desidera sottolineare che le garanzie essenziali europee si basano sulla giurisprudenza della Corte di giustizia dell'Unione europea (in appresso: CGUE) relativa agli articoli 7, 8, 47 e 52 della Carta dei diritti fondamentali dell'UE (in appresso: la Carta) e, se del caso, sulla giurisprudenza della Corte europea dei diritti dell'uomo (in appresso: CEDH) relativa all'articolo 8 della Convenzione europea dei diritti dell'uomo (in appresso: CEDU) che riguarda le questioni relative alle attività di sorveglianza negli Stati firmatari della CEDU[3].

3. L'aggiornamento del presente documento, originariamente redatto in risposta alla sentenza Schrems I[4], intende sviluppare ulteriormente le garanzie essenziali europee per tenere conto dei chiarimenti forniti dalla CGUE (e dalla CEDH) successivamente alla sua prima pubblicazione, in particolare nella fondamentale sentenza Schrems II[5].

4. Nella sentenza Schrems II, la CGUE ha dichiarato che l'esame della decisione 2010/87/UE della Commissione relativa alle clausole contrattuali tipo per il trasferimento di dati personali a responsabili del trattamento stabiliti in paesi terzi, alla luce degli articoli 7, 8 e 47 della Carta, non ha evidenziato alcun elemento idoneo a inficiarne la validità, ma ha condotto ad annullare la decisione relativa allo «scudo per la privacy» (Privacy Shield). La CGUE ha dichiarato che la decisione relativa allo «scudo per la privacy» è incompatibile con l'articolo 45, paragrafo 1, RGPD, alla luce degli articoli 7, 8 e 47 della Carta. La sentenza può quindi servire da esempio nel caso in cui le misure di sorveglianza in un paese terzo [in questo caso gli Stati Uniti con l'articolo 702 della Foreign Intelligence Surveillance Act (FISA) e il decreto presidenziale (Executive Order) 12333] non siano né sufficientemente limitate né soggette a un ricorso effettivo a disposizione degli interessati per far valere i loro diritti, come richiesto dal diritto dell'UE al fine di considerare il livello di protezione in un paese terzo come «sostanzialmente equivalente» a quello garantito all'interno dell'Unione europea ai sensi dell'articolo 45, paragrafo 1, del RGPD.

5. Le motivazioni che hanno condotto all'invalidazione della decisione relativa allo «scudo per la privacy» comportano conseguenze anche su altri strumenti di trasferimento[6]. Benché la Corte abbia interpretato l'articolo 46, paragrafo 1, del RGPD nel contesto della validità delle clausole contrattuali tipo, la sua interpretazione si applica a qualsiasi trasferimento verso paesi terzi che si fondi su uno qualsiasi degli strumenti di cui all'articolo 46 RGPD[7].

6. In ultima analisi, spetta alla CGUE giudicare se le ingerenze in un diritto fon-

damentale possano essere giustificate. Tuttavia, in assenza di un tale giudizio e in applicazione della giurisprudenza consolidata, le autorità competenti per la protezione dei dati personali sono tenute a valutare i singoli casi, d'ufficio o a seguito di un reclamo, e a deferire il caso a un tribunale nazionale se sospettano che il trasferimento non sia conforme all'articolo 45 in presenza di una decisione di adeguatezza, oppure a sospendere o vietare il trasferimento se ritengono che l'articolo 46 RGPD non possa essere rispettato e che non sia possibile garantire con altri mezzi la protezione richiesta dal diritto dell'UE per i dati trasferiti.

7. Le garanzie essenziali europee come aggiornate in questo documento intendono fornire elementi utili a valutare se misure di sorveglianza che consentono l'accesso ai dati personali da parte delle autorità pubbliche di un paese terzo, siano esse agenzie di sicurezza nazionale o autorità incaricate dell'applicazione della legge, possano configurare un'ingerenza giustificabile o meno.

8. Infatti, le garanzie essenziali europee fanno parte della valutazione da effettuare per stabilire se un paese terzo fornisca un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE, ma non mirano a definire di per sé tutti gli elementi necessari a ritenere che un paese terzo fornisce tale livello di protezione in conformità dell'articolo 45 del RGPD. Analogamente, esse non mirano a definire di per sé tutti gli elementi che potrebbero essere tenuti presenti nel valutare se il regime giuridico di un paese terzo impedisca all'esportatore e all'importatore di dati di assicurare le adeguate garanzie di cui all'articolo 46 del RGPD.

9. Pertanto, gli elementi forniti nel presente documento dovrebbero essere considerati come le garanzie essenziali da individuare in un paese terzo nel valutare l'ingerenza nei diritti al rispetto della vita privata e alla protezione dei dati derivante dalle misure di sorveglianza applicate in tale paese terzo, e non già un elenco di elementi atti a dimostrare che il regime giuridico di un paese terzo nel suo insieme fornisce un livello di protezione sostanzialmente equivalente.

10. L'articolo 6, paragrafo 3, del trattato sull'Unione europea stabilisce che i diritti fondamentali sanciti dalla CEDU fanno parte del diritto dell'UE in quanto principi generali. Tuttavia, come ricorda la CGUE nella sua giurisprudenza, la CEDU non costituisce, finché l'Unione europea non vi abbia aderito, un atto giuridico formalmente integrato nell'ordinamento giuridico dell'UE[8]. Pertanto, il livello di tutela dei diritti fondamentali richiesto dall'articolo 46, paragrafo 1, del RGPD deve essere determinato sulla base delle disposizioni di tale regolamento, lette alla luce dei diritti fondamentali sanciti dalla Carta. Ciò detto, ai sensi dell'articolo 52, paragrafo 3, della Carta, i diritti in essa contenuti che corrispondono ai diritti garantiti dalla CEDU hanno lo stesso significato e la stessa portata di quelli previsti da tale Convenzione e, di conseguenza, come ricordato dalla CGUE, occorre tener conto della giurisprudenza della CEDH in materia di diritti previsti anche dalla Carta dei diritti fondamentali dell'UE, in quanto livello minimo di protezione per interpretare i corrispondenti diritti della Carta[9]. Secondo l'ultimo comma dell'artico-

lo 52, paragrafo 3, della Carta, tuttavia, «[l]a presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa».

11. Pertanto, la sostanza delle garanzie essenziali continuerà a essere in parte basata sulla giurisprudenza della CEDH, nella misura in cui la Carta, come interpretata dalla CGUE, non preveda un livello di protezione più elevato che prescriva requisiti diversi dalla giurisprudenza della CEDH.

12. Il presente documento illustra il contesto e approfondisce ulteriormente le quattro garanzie essenziali europee.

2. INGERENZE NEI DIRITTI FONDAMENTALI

13. I diritti fondamentali al rispetto della vita privata e familiare, comprese le comunicazioni, e alla protezione dei dati personali sono stabiliti dagli articoli 7 e 8 della Carta e si applicano a tutti. L'articolo 8 stabilisce inoltre le condizioni per la liceità del trattamento dei dati personali e riconosce il diritto di accesso e di rettifica, oltre a imporre che tali norme siano soggette al controllo di un'autorità indipendente.

14. «[L]'operazione consistente nel far trasferire dati personali da uno Stato membro verso un paese terzo costituisce, in quanto tale, un trattamento di dati personali»[10]. Pertanto, gli articoli 7 e 8 della Carta si applicano a questa specifica operazione e la loro protezione si estende ai dati trasferiti, motivo per cui gli interessati i cui dati personali sono trasferiti verso un paese terzo devono poter beneficiare di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione europea[11].

15. Secondo la CGUE, quando il diritto fondamentale al rispetto della vita privata sancito dall'articolo 7 della Carta è pregiudicato, mediante il trattamento di dati personali di una persona, anche il diritto alla protezione dei dati è pregiudicato, in quanto tale trattamento rientra nell'ambito di applicazione dell'articolo 8 della Carta e, di conseguenza, deve necessariamente soddisfare il requisito di protezione dei dati previsto da tale articolo[12].

16. Pertanto, per quanto riguarda l'eventuale ingerenza nei diritti fondamentali ai sensi del diritto dell'UE, l'obbligo imposto ai fornitori di servizi di comunicazione elettronica [...] di conservare i dati relativi al traffico al fine di renderli, se del caso, accessibili alle autorità nazionali competenti solleva questioni riguardanti il rispetto degli articoli 7 e 8 della Carta[13]. Le stesse questioni si pongono anche per altre tipologie di trattamento di dati, come la loro trasmissione a soggetti diversi dagli utenti o l'accesso ai dati ai fini del loro utilizzo[14], che pertanto comportano un'ingerenza in tali diritti fondamentali. Inoltre, l'accesso di un'autorità pubblica ai dati costituisce un'ingerenza ulteriore, secondo una giurisprudenza consolidata[15].

17. Al fine di individuare un'ingerenza, non importa «che le informazioni relative alla vita privata di cui trattasi abbiano o meno natura sensibile, o che gli interessati abbiano o meno subito eventuali inconvenienti per effetto di tale ingerenza[16]». La CGUE ha inoltre sottolineato che è irrilevante[17] il fatto che i dati conservati siano stati o meno utilizzati successivamente.

18. Tuttavia, i diritti sanciti agli articoli 7 e 8 della Carta non appaiono come prerogative assolute, ma vanno considerati alla luce della loro funzione sociale[18].

19. La Carta prevede un test di necessità e proporzionalità per configurare le limitazioni ai diritti che tutela. L'articolo 52, paragrafo 1, della Carta specifica la portata delle possibili limitazioni ai diritti di cui agli articoli 7 e 8, affermando che «eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui».

20. La CGUE ha ribadito che la legislazione dell'UE che comporta un'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta «deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente tali dati contro il rischio di abusi», in particolare quando i dati personali sono sottoposti a trattamento automatico e «qualora esista un rischio considerevole di accesso illecito ai dati stessi[19]».

21. Secondo la CGUE, la tutela del diritto al rispetto della vita privata richiede che le deroghe e le restrizioni al diritto alla protezione dei dati «debbano operare entro i limiti dello stretto necessario». Inoltre, un obiettivo di interesse generale deve essere conciliato con i diritti fondamentali interessati dalla misura, «effettuando un equilibrato contemperamento» tra l'obiettivo e i diritti in questione[20].

22. Ne consegue che l'accesso, la conservazione e il successivo utilizzo di dati personali da parte delle autorità pubbliche nell'ambito delle misure di sorveglianza non devono superare i limiti dello stretto necessario, valutato alla luce della Carta, altrimenti «non [possono] essere [considerati giustificati] in una società democratica[21]».

23. Le quattro garanzie essenziali europee, così come sono sviluppate nel capitolo successivo, intendono specificare ulteriormente come valutare il livello di ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati nel contesto delle misure di sorveglianza applicate da autorità pubbliche di un paese terzo, in presenza di un trasferimento di dati personali, e quali requisiti giuridici devono essere conseguentemente in vigore per valutare se tali ingerenze siano accettabili ai sensi della Carta.

3. LE GARANZIE ESSENZIALI EUROPEE

24. In seguito all'analisi della giurisprudenza, l'EDPB ritiene che i requisiti giuridici applicabili per rendere giustificabili le limitazioni ai diritti alla protezione dei dati e al rispetto della vita privata riconosciuti dalla Carta possano essere riassunti in quattro garanzie essenziali europee:

A. Il trattamento deve basarsi su regole chiare, precise e accessibili
B. Devono essere dimostrate la necessità e la proporzionalità rispetto agli obiettivi legittimi perseguiti
C. Dovrebbe esistere un meccanismo di controllo indipendente
D. La persona deve poter accedere a mezzi di ricorso efficaci

25. Le garanzie si basano sui diritti fondamentali al rispetto della vita privata e alla protezione dei dati che si applicano a tutti, indipendentemente dalla nazionalità.

GARANZIA A - IL TRATTAMENTO DEVE BASARSI SU REGOLE CHIARE, PRECISE E ACCESSIBILI

26. Ai sensi dell'articolo 8, paragrafo 2, della Carta, i dati personali devono, in particolare, essere trattati «per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge[22]», come la CGUE ha ricordato nella sentenza Schrems II. Inoltre, ai sensi dell'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla stessa Carta all'interno dell'UE devono essere previste dalla legge. Pertanto, un'ingerenza giustificabile deve essere conforme alla legge.

27. Questa base giuridica dovrebbe definire regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e impongano alcune salvaguardie minime[23]. Inoltre, la Corte ha ricordato che «[la] normativa dev'essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale[24]». A questo proposito, la CGUE ha chiarito che la valutazione del diritto applicabile dei paesi terzi dovrebbe concentrarsi sulla possibilità riconosciuta alle persone di invocarlo e azionarlo dinanzi ai giudici[25]. La Corte indica pertanto che i diritti riconosciuti agli interessati devono essere azionabili; qualora alle persone non siano concessi diritti opponibili alle autorità pubbliche, il livello di protezione non può essere considerato sostanzialmente equivalente a quello derivante dalla Carta, contrariamente al requisito di cui all'articolo 45, paragrafo 2, lettera a), del RGPD[26].

28. Inoltre, la Corte ha sottolineato che il diritto applicabile deve indicare in quali circostanze e a quali condizioni possa essere adottata una misura che preveda il trattamento dei dati in questione[27] (cfr. *infra* alla garanzia B il rapporto fra tali requisiti e i principi di necessità e proporzionalità).

29. Inoltre, la CGUE ha indicato che «il requisito secondo cui qualsiasi limitazione nell'esercizio dei diritti fondamentali deve essere prevista dalla legge implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato[28]».

30. Infine, la Corte europea dei diritti dell'uomo «non ritiene che sussistano fondati motivi per giustificare l'applicazione di principi differenti alla questione dell'accessibilità e della chiarezza delle regole che governano, da un lato, l'intercettazione di comunicazioni individuali, e, dall'altro, i più generali pro-

grammi di sorveglianza[29]». La CEDH ha inoltre chiarito che la base giuridica dovrebbe comprendere almeno una definizione delle categorie di persone che potrebbero essere soggette a sorveglianza, un limite alla durata della misura, la procedura da seguire per l'esame, l'utilizzo e la conservazione dei dati ottenuti e le precauzioni da adottare nella comunicazione dei dati ad altre parti[30].

31. Infine, l'ingerenza deve essere prevedibile nei suoi effetti sulla persona, al fine di garantire una protezione adeguata ed efficace contro le ingerenze arbitrarie e il rischio di abusi. Di conseguenza, il trattamento deve fondarsi su una base giuridica precisa, chiara ma anche accessibile (cioè pubblica)[31]. La CEDH, in merito a tale questione, ha ricordato nel caso Zakharov che «la nozione di "prevedibilità" nel contesto dell'intercettazione delle comunicazioni non può essere interpretata secondo gli stessi parametri utilizzati in molti altri campi». Ha precisato che nel contesto delle misure segrete di sorveglianza, quali l'intercettazione delle comunicazioni, «la prevedibilità non può significare che una persona debba essere in grado di prevedere quando le autorità potrebbero intercettare le sue comunicazioni in modo da poter adattare il suo comportamento di conseguenza». Tuttavia, considerando che in questo tipo di situazione i rischi di arbitrarietà sono evidenti, «è essenziale avere regole chiare e dettagliate sull'intercettazione delle conversazioni telefoniche, tanto più che la tecnologia disponibile per tale scopo diventa sempre più sofisticata. Il diritto nazionale deve essere sufficientemente chiaro da fornire ai cittadini un'indicazione adeguata in merito alle circostanze in cui e alle condizioni alle quali le autorità pubbliche possono ricorrere a tali misure»[32].

GARANZIA B - DEVONO ESSERE DIMOSTRATE LA NECESSITÀ E LA PROPORZIONALITÀ RISPETTO AGLI OBIETTIVI LEGITTIMI PERSEGUITI

32. In conformità del primo comma dell'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla stessa Carta devono rispettare il contenuto essenziale di detti diritti e libertà. Ai sensi del secondo comma dell'articolo 52, paragrafo 1, della Carta, nel rispetto del principio di proporzionalità, possono essere apportate limitazioni a tali diritti e libertà solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui[33].

33. Per quanto riguarda il **principio di proporzionalità**, la Corte ha dichiarato, in relazione alle legislazioni degli Stati membri, che la giustificabilità di una limitazione dei diritti al rispetto della vita privata e alla protezione dei dati deve essere valutata, da un lato, misurando la **gravità dell'ingerenza** che tale limitazione comporta[34] e, dall'altro, verificando che l'**importanza dell'obiettivo di interesse generale** perseguito attraverso tale limitazione sia proporzionata alla suddetta gravità[35].

34. In La Quadrature du Net et al., si può osservare che la CGUE ha stabilito, in relazione al diritto di uno Stato membro e non al diritto di un paese terzo, che

l'obiettivo di salvaguardia della sicurezza nazionale è, per la sua importanza, idoneo a giustificare misure che comportino ingerenze nei diritti fondamentali più gravi di quelle che potrebbero essere giustificate da altri obiettivi, come la lotta alla criminalità. Essa ha tuttavia constatato che ciò vale fintantoché ricorrano circostanze sufficientemente concrete tali da consentire di ritenere che lo Stato interessato si trovi dinanzi a una minaccia grave alla sicurezza nazionale, che si dimostri reale e attuale o prevedibile, e a condizione che siano soddisfatti gli altri requisiti di cui all'articolo 52, paragrafo 1, della Carta[36].

35. A tal proposito, secondo la giurisprudenza consolidata della Corte, le deroghe e le limitazioni alla protezione dei dati personali devono essere applicate solo nella misura strettamente necessaria[37]. Per soddisfare tale requisito, oltre a stabilire regole chiare e precise che disciplinano la portata e l'applicazione della misura in questione, la legislazione deve imporre alcune salvaguardie minime in modo che le persone i cui dati sono trasferiti dispongano di garanzie sufficienti a proteggere efficacemente i loro dati personali contro il rischio di abusi. «In particolare, essa deve indicare in quali circostanze e a quali condizioni possa essere adottata una misura che prevede il trattamento di siffatti dati, garantendo così che l'ingerenza sia limitata allo stretto necessario. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatizzato»[38].

36. In Schrems II, la CGUE ha sottolineato che la legislazione di un paese terzo che non indica alcuna limitazione al potere da essa conferito di attuare programmi di sorveglianza ai fini dell'intelligence esterna non può assicurare un livello di protezione sostanzialmente equivalente a quello garantito dalla Carta. Infatti, secondo la giurisprudenza, una base giuridica che consente ingerenze nei diritti fondamentali, al fine di soddisfare i requisiti del principio di proporzionalità, deve definire essa stessa la portata della limitazione dell'esercizio del diritto di cui trattasi[39].

37. Per quanto riguarda il **principio di necessità**, la CGUE ha chiarito che le legislazioni «che autorizzano, su base generalizzata, la conservazione dei dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione Europea [...] senza che sia fatta alcuna distinzione, limitazione o eccezione alla luce dell'obiettivo perseguito e senza che sia stabilito un criterio oggettivo per determinare i limiti dell'accesso delle autorità pubbliche ai dati e del loro successivo utilizzo, per finalità specifiche, strettamente limitate e atte a giustificare l'ingerenza che l'accesso ai dati e il loro utilizzo comportano», non rispettano tale principio[40]. In particolare, le leggi che consentono alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche devono essere ritenute pregiudizievoli del contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta[41].

38. Analogamente, ma nel valutare il diritto di uno Stato membro e non quello di un paese terzo, la CGUE ha affermato, nella sentenza La Quadrature du Net et al., che «una normativa che preveda una conservazione dei dati personali deve sempre rispondere a criteri oggettivi, che pongano un rapporto tra i

dati personali da conservare e l'obiettivo perseguito»[42]. Nello stesso contesto, nella sentenza Privacy International, ha affermato inoltre che il legislatore «deve fondarsi su criteri oggettivi per definire le circostanze e le condizioni in cui dev'essere concesso alle autorità nazionali competenti l'accesso ai dati di cui trattasi»[43].

GARANZIA C - MECCANISMO DI CONTROLLO INDIPENDENTE

39. L'EDPB ricorda che un'ingerenza avviene al momento della raccolta dei dati, ma anche al momento dell'accesso ai dati da parte di un'autorità pubblica in vista di un trattamento ulteriore. La CEDH ha specificato più volte che qualsiasi ingerenza nel diritto al rispetto della vita privata e alla protezione dei dati deve essere soggetta a un sistema di controllo efficace, indipendente e imparziale che deve essere previsto da un giudice o da un altro organo indipendente[44] (ad esempio un'autorità amministrativa o un organo parlamentare). Il controllo indipendente dell'attuazione delle misure di sorveglianza è stato preso in considerazione anche dalla CGUE nella sentenza Schrems II[45].

40. La CEDH precisa che, se da un lato l'autorizzazione preventiva (giudiziaria) delle misure di sorveglianza costituisce un requisito importante contro l'arbitrarietà, dall'altro occorre anche tener conto del funzionamento concreto del sistema di intercettazione, compresi i meccanismi tesi ad assicurare l'esercizio equilibrato del potere, nonché dell'esistenza o meno di un effettivo abuso[46]. Nel caso Schrems II, la CGUE ha tenuto conto anche dell'ambito della vigilanza affidata al meccanismo di controllo, che non comprendeva le singole misure di sorveglianza[47].

41. Per quanto riguarda il diritto degli Stati membri, la CGUE ha individuato una serie di misure che sono conformi al diritto dell'UE solo qualora siano soggette a un controllo effettivo da parte di un tribunale o di un'autorità amministrativa indipendente la cui decisione sia vincolante. Lo scopo di tale controllo è verificare l'esistenza di una situazione che giustifichi la misura in questione, e il rispetto delle condizioni e delle garanzie che devono essere previste[48]. Per quanto riguarda la raccolta in tempo reale dei dati relativi al traffico e all'ubicazione, l'esame dovrebbe consentire di verificare ex ante, tra l'altro, se essa sia autorizzata solo nei limiti dello stretto necessario. In caso di emergenza debitamente giustificata, le misure possono essere applicate senza tale controllo preventivo; tuttavia, la Corte richiede comunque che il controllo successivo intervenga tempestivamente[49].

42. Per quanto riguarda l'indipendenza dei meccanismi di controllo in relazione alle misure di sorveglianza, si può tener conto delle conclusioni della CGUE in merito all'indipendenza di un organismo nell'esercizio di mezzi di ricorso (cfr. *infra* alla garanzia D). Inoltre, la giurisprudenza della CEDH può offrire ulteriori elementi. Quest'ultima, infatti, si è espressa nel senso di preferire che il controllo sia affidato a un giudice. Tuttavia, non è escluso che un altro organismo possa essere incaricato di tale controllo, «purché sia sufficientemente indipendente dall'esecutivo»[50] e «dalle autorità che effettuano la

sorveglianza, e [sia] dotato di poteri e competenze sufficienti per esercitare un controllo efficace e continuo»[51]. La CEDH ha aggiunto che occorre tenere in considerazione «le modalità di nomina e lo status giuridico dei membri dell'organismo di controllo»[52] nel valutarne l'indipendenza. Ciò include «persone qualificate a ricoprire una funzione giurisdizionale, nominate dal parlamento o dal Primo ministro. Al contrario, un ministro dell'Interno, che non solo era di nomina politica e membro dell'esecutivo, ma era direttamente coinvolto nella messa in funzione di misure speciali di sorveglianza, è stato giudicato non sufficientemente indipendente»[53]. La CEDH «osserva inoltre che è essenziale che l'organo di vigilanza abbia accesso a tutti i documenti pertinenti, compreso il materiale riservato»[54]. Infine, la CEDH prende in considerazione «se le attività dell'organo di controllo siano soggette al controllo pubblico»[55].

GARANZIA D - LA PERSONA DEVE POTER ACCEDERE A MEZZI DI RICORSO EFFICACI

43. L'ultima garanzia essenziale europea è legata ai diritti di ricorso della persona, che deve poter disporre di un mezzo di ricorso efficace per soddisfare i suoi diritti quando ritiene che essi non siano o non siano stati rispettati. Nella sentenza Schrems I la CGUE ha spiegato che «una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta. Infatti, l'articolo 47, primo comma, della Carta esige che ogni individuo i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati abbia diritto ad un ricorso effettivo dinanzi ad un giudice, nel rispetto delle condizioni previste in tale articolo»[56].

44. Nel valutare il diritto di uno Stato membro che consente la raccolta in tempo reale dei dati relativi al traffico e all'ubicazione, la Corte ha ritenuto che la comunicazione alla persona interessata sia necessaria «per consentire a dette persone di esercitare i loro diritti, derivanti dagli articoli 7 e 8 della Carta, di chiedere l'accesso ai propri dati personali costituenti l'oggetto di tali misure e, se del caso, la rettifica o la cancellazione degli stessi, nonché di proporre, conformemente all'articolo 47, primo comma, della Carta, un ricorso effettivo dinanzi a un giudice»[57]. Tuttavia, ha anche riconosciuto che la comunicazione alle persone i cui dati sono stati raccolti o analizzati deve avvenire soltanto nella misura e a partire dal momento in cui essa non può più compromettere lo svolgimento dei compiti che sono di pertinenza delle specifiche autorità[58].

45. Anche per la CEDH la questione dell'esistenza di un mezzo di ricorso efficace è indissolubilmente legata alla comunicazione alla persona dell'applicazione di una misura di sorveglianza una volta terminata la sorveglianza stessa. In particolare, la Corte ha ritenuto che «in linea di principio vi sono scarse possibilità di ricorso al giudice da parte della persona interessata, a meno che

quest'ultima non sia informata delle misure adottate a sua insaputa e possa quindi contestarne la legalità a posteriori o, in alternativa, a meno che chiunque sospetti che le sue comunicazioni siano o siano state intercettate possa rivolgersi al giudice, di modo che la competenza del giudice non dipenda dalla comunicazione al soggetto intercettato dell'avvenuta intercettazione delle sue comunicazioni»[59]. La CEDH ha quindi riconosciuto che in alcuni casi potrebbe non esserci alcuna comunicazione, ma è necessario prevedere sempre un mezzo di ricorso efficace. In questo caso, la Corte ha chiarito, ad esempio nella causa Kennedy, che un tribunale offre sufficienti possibilità di ricorso qualora soddisfi una serie di criteri, vale a dire sia un organo indipendente e imparziale, che abbia adottato un proprio regolamento interno, sia composto da membri che devono ricoprire o aver ricoperto alte cariche giudiziarie o essere avvocati esperti, e non vi sia alcuna soglia di ordine probatorio da superare per poterlo adire[60]. Nell'esaminare le denunce dei singoli, il tribunale deve avere accesso a tutte le informazioni pertinenti[61], compreso il materiale riservato. Infine, dovrebbe avere il potere di disporre rimedi in caso di inosservanza[62].

46. L'articolo 47 della Carta fa riferimento a un tribunale, anche se nelle versioni linguistiche diverse dall'inglese la preferenza è data alla parola «giudice»[63], mentre la CEDU si limita a prevedere l'obbligo per gli Stati membri di garantire che «ogni persona i cui diritti e le cui libertà siano stati violati, [abbia] diritto a un ricorso effettivo davanti a un'istanza nazionale»[64], che non deve necessariamente essere un'autorità giudiziaria[65].

47. La CGUE, nel contesto della sentenza Schrems II, nel valutare l'adeguatezza del livello di protezione di un paese terzo, ha ribadito che «i singoli devono disporre della possibilità di esperire mezzi di ricorso dinanzi a un giudice indipendente e imparziale al fine di avere accesso a dati personali che li riguardano, o di ottenere la rettifica o la soppressione di tali dati»[66]. Nello stesso contesto, la CGUE ritiene che un'efficace protezione giudiziaria contro tali interferenze possa essere assicurata non solo da un tribunale, ma anche da un organo[67] che offra garanzie sostanzialmente equivalenti a quelle richieste dall'articolo 47 della Carta. Nella sentenza Schrems II, la CGUE ha sottolineato che l'indipendenza del giudice o dell'organo deve essere assicurata, in particolare nei confronti del potere esecutivo, con tutte le garanzie necessarie, anche per quanto riguarda le condizioni di revoca o annullamento della nomina[68], e che i poteri che dovrebbero essere concessi a un giudice devono essere conformi ai requisiti dell'articolo 47 della Carta. A tale riguardo, all'organo[69] deve essere conferito il potere di adottare decisioni vincolanti per i servizi di intelligence, nel rispetto di garanzie giuridiche che gli interessati possano invocare[70].

4. OSSERVAZIONI CONCLUSIVE

48. Le quattro garanzie essenziali europee sono da considerarsi elementi fondamentali per valutare il livello di ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati. Esse non dovrebbero essere va-

lutate in modo indipendente, essendo in realtà strettamente interconnesse, bensì complessivamente, esaminando la legislazione pertinente in relazione alle misure di sorveglianza, al livello minimo di garanzie per la protezione dei diritti degli interessati e ai mezzi di ricorso previsti dalla legislazione nazionale del paese terzo.

49. Tali garanzie richiedono un certo grado di interpretazione, soprattutto perché la legislazione del paese terzo non deve necessariamente essere identica al quadro giuridico dell'UE.

50. Come ha affermato la Corte europea dei diritti dell'uomo nel caso Kennedy, «la valutazione dipende da tutte le circostanze del caso, come la natura, la portata e la durata delle possibili misure, i requisiti necessari per disporne l'adozione, le autorità competenti ad autorizzarle, applicarle e controllarle e la tipologia dei mezzi di ricorso previsti dal diritto nazionale»[71].

51. Di conseguenza, la valutazione delle misure di sorveglianza dei paesi terzi rispetto alle garanzie essenziali europee può portare a due conclusioni:

- la legislazione del paese terzo in questione non soddisfa i requisiti delle garanzie essenziali europee: in questo caso, la legislazione del paese terzo non offrirebbe un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE;
- la legislazione del paese terzo in questione soddisfa le garanzie essenziali europee.

52. Nel valutare l'adeguatezza del livello di protezione, ai sensi dell'articolo 45 del RGPD, la Commissione dovrà valutare se le garanzie essenziali europee siano soddisfatte nel quadro degli elementi da considerare per garantire che la legislazione del paese terzo nel suo insieme offra un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE.

53. Quando gli esportatori di dati si affidano, insieme agli importatori di dati, ad adeguate garanzie ai sensi dell'articolo 46 del RGPD, tenuto conto dei requisiti della legislazione dei paesi terzi specificamente applicabili ai dati trasferiti, essi dovrebbero garantire che sia effettivamente raggiunto un livello di protezione sostanzialmente equivalente. In particolare, qualora la legislazione del paese terzo non sia conforme ai requisiti delle garanzie essenziali europee, ciò comporterebbe garantire che la legislazione in questione non pregiudichi le garanzie e le salvaguardie relative al trasferimento affinché sia comunque assicurato un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE.

54. L'EDPB ha pubblicato ulteriori linee guida e raccomandazioni da prendere in considerazione nel procedere alla valutazione, a seconda dello strumento di trasferimento da utilizzare e della necessità di fornire garanzie adeguate, comprese, se del caso, misure supplementari[72].

55. Inoltre, va osservato che le garanzie essenziali europee si basano su quanto previsto dalla legge. L'EDPB sottolinea che le garanzie essenziali europee sono fondate sui diritti fondamentali, i quali si applicano a tutti, indipendentemente dalla nazionalità.

56. L'EDPB ribadisce che le garanzie essenziali europee sono uno standard di riferimento per valutare l'ingerenza che le misure di sorveglianza di paesi terzi comportano nel contesto dei trasferimenti internazionali di dati. Tali standard derivano dal diritto dell'UE e dalla giurisprudenza della CGUE e della CEDH, che è vincolante per gli Stati membri.

NOTE

[1] Il presente documento non riguarda i trasferimenti o le condivisioni successive che ricadano nell'ambito della direttiva "polizia e giustizia" [direttiva (UE) 2016/680].

[2] Nel presente documento, con «Stati membri» ci si riferisce agli «Stati membri del SEE».

[3] Nelle presenti raccomandazioni, il termine «diritti fondamentali» deriva dalla Carta dei diritti fondamentali dell'UE. Tuttavia, esso è utilizzato anche per ricomprendere i «diritti umani» inclusi nella Convenzione europea dei diritti dell'uomo.

[4] Sentenza della CGUE del 6 ottobre 2015, Maximillian Schrems contro Data Protection Commissioner, causa C-362/14, EU:C:2015:650 (in appresso: Schrems I).

[5] Sentenza della CGUE del 16 luglio 2020, Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems, causa C-311/18, ECLI:EU:C:2020:559 (in appresso: Schrems II).

[6] Cfr. § 105 di Schrems II.

[7] Cfr. § 92 di Schrems II.

[8] Cfr. § 98 di Schrems II.

[9] Cfr. § 124 delle cause riunite C-511/18, C-512/18 e C-520/18, La Quadrature du Net et al. (in appresso: La Quadrature du Net et al.).

[10] CGUE, Schrems II, § 83.

[11] CGUE, Schrems II, § 96.

[12] CGUE, Schrems II, §§ 170-171.

[13] CGUE, causa C-623/17, Privacy International (in appresso: Privacy International), § 60.

[14] CGUE, Privacy International, § 61.

[15] CEDH, Leander, § 48; CEDH, Rotaru, § 46; CGUE, Digital Rights Ireland, § 35.

[16] CGUE, Schrems II, § 171, compresa la giurisprudenza citata.

[17] CGUE, Schrems II, § 171, compresa la giurisprudenza citata.

[18] CGUE, Privacy International, § 63.

[19] CGUE, Privacy International, § 68 e giurisprudenza ivi menzionata.

[20] CGUE, Privacy International, § 67 e giurisprudenza ivi menzionata.

[21] CGUE, Privacy International, § 81.

[22] Cfr. § 173 di Schrems II.

[23] Cfr. § 175 e § 180 di Schrems II e il parere 1/15 [accordo UE -Canada sul codice di prenotazione (Passenger Name Record, PNR)] del 26 luglio 2017, § 139 e la giurisprudenza citata.

[24] Cfr. § 68 di Privacy International – Si fa notare che nella versione francese della sentenza la Corte usa la parola «réglementation», che è più ampia rispetto ai soli atti del Parlamento.

[25] Cfr. § 181 di Schrems II; in tale paragrafo la CGUE si riferisce alla direttiva presidenziale 28 (Presidential Policy directive 28) degli Stati Uniti.

[26] Cfr. § 181 di Schrems II.

[27] Cfr. § 68 di Privacy International, in relazione al diritto degli Stati membri.

[28] Cfr. Schrems II, § 175 e la giurisprudenza citata, nonché Privacy International, § 65.

[29] CEDH, Liberty, § 63.

[30] CEDH, Weber e Saravia, § 95.

[31] CEDH, Malone, §§ 65 e 66.

[32] CEDH, Zakharov, § 229.

[33] Schrems II, § 174.

[34] In tale contesto, il giudice ha rilevato, ad esempio, che «l'ingerenza derivante dalla raccolta in tempo reale dei dati che consentono di localizzare un'apparecchiatura terminale risulta particolarmente grave, dato che tali dati forniscono alle autorità nazionali competenti uno strumento di controllo preciso e permanente degli spostamenti degli utenti dei telefoni mobili [...]» (La Quadrature du Net et al., § 187, compresa la giurisprudenza citata).

[35] La Quadrature du Net et al., § 131.

[36] §§ 136 e 137. Cfr. anche Privacy International: come precisato dalla Corte, tali minacce possono essere distinte, per la loro natura e la loro particolare gravità, dal rischio generale che si verifichino tensioni o perturbazioni, anche gravi, della pubblica sicurezza. § 75. Ad esempio, nella causa La Quadrature du Net et al., la Corte ha rilevato che l'analisi automatizzata dei dati relativi al traffico e all'ubica-

zione appare come un'ingerenza particolarmente grave in quanto riguarda in modo generalizzato e indifferenziato i dati delle persone che si avvalgono dei mezzi di comunicazione elettronica; una tale misura può soddisfare il requisito di proporzionalità solo in situazioni nelle quali lo Stato membro interessato si trovi di fronte ad una minaccia grave per la sicurezza nazionale che risulti reale e attuale o prevedibile e, in particolare, a condizione che la durata di tale conservazione sia limitata allo stretto necessario (§§ 174-177).

[37] Schrems II, § 176, compresa la giurisprudenza citata.

[38] Schrems II, § 175.

[39] Schrems II, § 180.

[40] Schrems I, § 93 e ulteriori riferimenti. Cfr., ma in relazione al diritto di uno Stato membro e non a quello di un paese terzo, Privacy International, § 71, inclusa la giurisprudenza citata. In questo caso, la Corte ha affermato che la legislazione di uno Stato membro che impone ai fornitori di servizi di comunicazione elettronica di comunicare i dati relativi al traffico e all'ubicazione alle agenzie di sicurezza e di intelligence mediante una trasmissione generale e indifferenziata supera i limiti dello stretto necessario e non può essere considerata giustificata, in una società democratica, come richiesto dalla direttiva relativa alla vita privata e alle comunicazioni elettroniche, letta alla luce della Carta (§ 81).

[41] Schrems I, § 94.

[42] La Quadrature du Net et al., § 133. In tale contesto, la Corte ha confermato che le misure legislative che prevedono, in via preventiva, la conservazione generale e indifferenziata dei dati relativi al traffico e all'ubicazione sono vietate dalla direttiva relativa alla vita privata e alle comunicazioni elettroniche, letta alla luce della Carta. Per contro, la Corte ha stabilito che, in situazioni di grave minaccia alla sicurezza nazionale che si dimostri reale e presente o prevedibile, il legislatore può consentire, per la salvaguardia della sicurezza nazionale, il ricorso a un'istruzione che imponga ai fornitori di servizi di comunicazione elettronica di conservare, in modo generale e indifferenziato, i dati relativi al traffico e all'ubicazione. Tale misura deve tuttavia soddisfare condizioni specifiche. In particolare, l'istruzione può essere impartita solo per un periodo di tempo limitato allo stretto necessario, che può essere prorogato se tale minaccia persiste (§ 168).

[43] Privacy International, § 78, compresa la giurisprudenza citata. Nella causa Privacy International, per quanto riguarda l'accesso di un'autorità ai dati personali forniti ai sensi della legge di uno Stato membro, la Corte ha stabilito che «un accesso generale a tutti i dati conservati, in mancanza di qualunque nesso, anche indiretto, con la finalità perseguita, non può essere considerato limitato allo stretto necessario» (§ 77-78).

[44] CEDH, Klass, §§ 17, 51.

[45] Schrems II, §§ 179, 183.

[46] CEDH, Big Brother Watch in appello, §§ 319-320.

[47] Schrems II, § 179.

[48] CGUE, La Quadrature du Net et al., §§ 168, 189.

[49] CGUE, La Quadrature du Net et al., § 189.

[50] CEDH, Zakharov, § 258, Iordachi et al. C. Moldavia, §§ 40 e 51, e Dumitru Popescu c. Romania, §§ 70-73.

[51] CDEH, Klass § 56 e Big Brother Watch in appello, § 318.

[52] CEDH, Zakharov, § 278.

[53] CEDH, Zakharov, § 278.

[54] CEDH, Zakharov, § 281.

[55] CEDH, Zakharov, § 283.

[56] CGUE, Schrems I, § 95.

[57] Cfr. § 190 di La Quadrature du Net et al. E CGUE, parere 1/15, § 220.

[58] Cfr. § 191 di La Quadrature du Net et al..

[59] CEDH, Zakharov, § 234.

[60] CEDH, Kennedy, § 190.

[61] L'EDPB osserva che il Commissario per i diritti umani del Consiglio d'Europa ritiene che la cosiddetta regola dei «terzi», in base alla quale le agenzie di intelligence di un paese che forniscono dati alle agenzie di intelligence di un altro paese possono imporre agli organismi riceventi l'obbligo di non divulgare i dati trasferiti a terzi, non dovrebbe applicarsi agli organismi di controllo per non compromettere la possibilità di un ricorso efficace (Issue Paper on Democratic and effective oversight of national security services).

[62] CEDH, Kennedy, § 167.

[63] La parola «tribunale» è ad esempio tradotta come «Gericht» in tedesco e «gerecht» in olandese.

[64] Articolo 13 della CEDU

[65] CEDH, Klass § 67.

[66] Cfr. § 194 di Schrems II.

[67] Cfr. § 197 di Schrems II, in cui la Corte usa espressamente tale termine.

[68] Cfr. § 195 di Schrems II.

[69] Cfr. § 197 di Schrems II, in cui la Corte usa espressamente

tale termine.

[70] Cfr. § 196 di Schrems II.

[71] CEDH, Kennedy, § 153.

[72] Adequacy Referential WP 254 rev.01, riveduto e adottato il 6 febbraio 2018; raccomandazioni 01/2020 dell'EDPB relative alle misure che integrano gli strumenti di trasferimento per garantire il rispetto del livello di protezione dei dati personali nell'UE, 10 novembre 2020.

Raccomandazioni 1/2021 sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie

Adottate il 2 febbraio 2021

Cronologia delle versioni

Versione 1.1	6 luglio 2021	Modifica di formattazione
Versione 1.0	2 febbraio 2021	Adozione delle raccomandazioni

Indice

1 Introduzione

2. Concetto di adeguatezza

3. Aspetti procedurali per i riscontri relativi all'adeguatezza a norma della LED

4. Norme Ue concernenti l'adeguatezza nella cooperazione di polizia e nella cooperazione giudiziaria in materia penale

A. Principi generali e garanzie

a) Nozioni

b) Liceità e correttezza del trattamento dei dati personali

c) Il principio della limitazione delle finalità

d) Condizioni specifiche per l'ulteriore trattamento per finalità diverse

e) Il principio della minimizzazione dei dati

f) Il principio dell'esattezza dei dati

g) Il principio della conservazione dei dati

h) Il principio della sicurezza e della riservatezza

i) Il principio della trasparenza (articolo 13; considerando 26, 39, 42, 43, 44, 46)

j) Il diritto di accesso, rettifica e cancellazione (articoli 14 e 16)

k) Limitazioni dei diritti degli interessati

l) Limitazione relativa ai trasferimenti successivi (articolo 35, considerando 64 e 65)

m) Principio di responsabilizzazione

B. Esempi di principi supplementari da applicare a tipi specifici di trattamento

a) Categorie particolari di dati

b) Processo decisionale automatizzato e profilazione

c) Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

C. Meccanismi di procedura e applicazione

a) Autorità di controllo indipendente competente

b) Attuazione efficace delle norme in materia di protezione dei dati

c) il sistema di protezione dei dati deve facilitare l'esercizio dei diritti dell'interessato

d) Il sistema di protezione dei dati deve prevedere meccanismi di ricorso adeguati

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 51, paragrafo 1, lettera b), della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio[1],

visti gli articoli 12 e 22 del proprio regolamento interno,

HA ADOTTATO LE SEGUENTI RACCOMANDAZIONI:

1. INTRODUZIONE

1. Il gruppo di lavoro Articolo 29 ha pubblicato un documento di lavoro[2] sui criteri di riferimento per l'adeguatezza ai sensi del regolamento generale della protezione dei dati[3]. Tale documento di lavoro è stato approvato dal comitato europeo per la protezione dei dati (il "comitato") in occasione della sua prima sessione plenaria.
2. Come affermato nella dichiarazione n. 21 allegata al trattato di Lisbona, potrebbero rivelarsi necessarie, in considerazione della specificità dei settori in questione, norme specifiche sulla protezione dei dati personali e sulla libera circolazione di tali dati nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia, in base all'articolo 16 del trattato sul funzionamento dell'Unione europea (TFUE).
3. Su questa base, il legislatore dell'UE ha adottato la direttiva (UE) 2016/680 (la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, di seguito "LED") che stabilisce le norme specifiche in materia di trattamento dei dati personali da parte delle autorità competenti a fini di **prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica**.
4. Tale direttiva stabilisce i motivi che consentono il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale in tale contesto. Uno dei motivi sul quale si può basare tale trasferimento è la decisione della Commissione europea attestante che il paese terzo o l'organizzazione internazionale in questione garantisce un livello di protezione adeguato.
5. Mentre il documento di lavoro WP254 rev.01 sui criteri di riferimento per l'adeguatezza mira a fornire orientamenti alla Commissione europea in merito al livello di protezione dei dati nei paesi terzi e nelle organizzazioni internazionali ai sensi del regolamento generale sulla protezione dei dati, il presente documento mira a fornire orientamenti analoghi nel quadro della LED. In tale contesto stabilisce i principi fondamentali in materia di protezione dei dati che devono essere presenti nel quadro giuridico di un paese terzo o di un'organizzazione internazionale per garantire un'equivalenza essenziale rispetto al quadro dell'UE nell'ambito di applicazione della LED (ossia per il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali). Inoltre, può fornire orientamenti ai paesi terzi e alle organizzazioni internazionali interessati a ottenere l'adeguatezza.
6. Il presente documento si concentra esclusivamente sulle decisioni di adeguatezza. Si tratta di atti di esecuzione della Commissione europea a norma dell'articolo 36, paragrafo 3, della LED.

2. CONCETTO DI ADEGUATEZZA

7. La LED stabilisce le norme per il trasferimento di dati personali verso paesi terzi e organizzazioni internazionali nella misura in cui tali trasferimenti rientrano nel suo ambito di applicazione. Le norme sui trasferimenti internazionali di dati personali sono stabilite nel capo V di tale direttiva, in particolare negli articoli da 35 a 39.

8. Ai sensi dell'articolo 36 della LED, il trasferimento di dati verso un paese terzo o un'organizzazione internazionale può avvenire se un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato. Dalla giurisprudenza della Corte di giustizia dell'Unione europea[4] si evince che tale disposizione deve essere letta alla luce dell'articolo 35 della LED, intitolato "Principi generali per il trasferimento di dati personali", il quale stabilisce che "[t]utte le disposizioni del [capo V di tale direttiva] sono applicate al fine di assicurare che il livello di protezione delle persone fisiche assicurato dalla presente direttiva non sia pregiudicato".

9. Se la Commissione europea ha deciso che è garantito un tale livello di protezione adeguato, i trasferimenti di dati personali verso tale paese terzo, territorio, settore od organizzazione internazionale possono avere luogo senza specifiche autorizzazioni, tranne nel caso in cui un altro Stato membro presso cui sono stati ottenuti i dati debba autorizzare il trasferimento, come previsto dagli articoli 35 e 36 e dal considerando 66 della LED. Ciò non pregiudica la necessità che il trattamento dei dati da parte delle autorità degli Stati membri interessati debba essere conforme alle disposizioni nazionali adottate a norma della direttiva (UE) 2016/680.

10. Il concetto di "livello di protezione adeguato", che già esisteva ai sensi della direttiva 95/46[5] e della decisione quadro 2008/977/GAI del Consiglio[6], è stato ulteriormente sviluppato dalla Corte di giustizia dell'Unione europea in questo contesto e, di recente, nel quadro del regolamento generale sulla protezione dei dati.

11. Come specificato dalla Corte di giustizia dell'Unione europea, sebbene il livello di protezione nel paese terzo debba essere sostanzialmente equivalente a quello garantito nell'UE, "gli strumenti dei quali tale paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all'interno dell'Unione" ma "tali strumenti devono cionondimeno rivelarsi efficaci, nella prassi"[7]. Il livello di adeguatezza non richiede pertanto di riprodurre punto per punto la legislazione dell'UE, bensì di stabilire i requisiti sostanziali - di base - di tale legislazione.

12. In tale contesto la Corte ha altresì chiarito che una decisione di adeguatezza della Commissione dovrebbe contenere una dichiarazione quanto all'esistenza, nel paese terzo, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso tale paese terzo, ingerenze che entità statali di tale paese sarebbero *autorizzate* a compiere laddove perseguano obiettivi legittimi, come la sicurezza nazionale[8].

13. Lo scopo delle decisioni di adeguatezza emesse dalla Commissione europea è confermare formalmente con effetto vincolante per gli Stati membri[9], comprese le loro autorità competenti per la protezione dei dati personali[10], che il livello di protezione dei dati in un paese terzo o in un'organizzazione internazionale è sostanzialmente equivalente al livello di protezione dei dati all'interno dell'Unione europea. Il paese terzo dovrebbe offrire garanzie atte ad assicurare un adeguato livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione, in particolare qualora i dati siano trattati in uno o più settori specifici[11].

14. L'adeguatezza può essere conseguita anche attraverso una combinazione di diritti degli interessati e obblighi in capo a chi effettua il trattamento o esercita il controllo sul trattamento, e il controllo da parte di organismi indipendenti. Le norme in materia di protezione dei dati, tuttavia, sono efficaci solo se sono azionabili e sono rispettate nella pratica. È pertanto necessario considerare non solo il contenuto delle norme applicabili ai dati personali trasferiti in un paese terzo o un'organizzazione internazionale, ma anche il sistema in atto per garantirne l'efficacia. La presenza di meccanismi di applicazione efficienti è di fondamentale importanza per garantire l'efficacia delle norme sulla protezione dei dati[12].

3. ASPETTI PROCEDURALI PER I RISCONTRI RELATIVI ALL'ADEGUATEZZA A NORMA DELLA LED

15. Al fine di adempiere il proprio compito di fornire consulenza alla Commissione europea a norma dell'articolo 51, paragrafo 1, lettera g), della LED, il comitato deve ricevere tutta la documentazione necessaria, compresa la corrispondenza pertinente e le conclusioni tratte dalla Commissione europea. È assolutamente necessario che tutti i documenti pertinenti siano trasmessi con sufficiente anticipo, tradotti in inglese, al comitato per consentire discussioni informate e utili prima dell'adozione definitiva delle decisioni di adeguatezza. Se il quadro giuridico è complesso, dovrebbero essere fornite anche eventuali relazioni sul livello di protezione dei dati nel paese terzo o nell'organizzazione internazionale. In ogni caso, le informazioni fornite dalla Commissione europea dovrebbero essere esaustive e consentire al comitato di valutare l'analisi condotta dalla Commissione in merito al livello di protezione dei dati nel paese terzo o presso l'organizzazione internazionale.

16. Il comitato fornirà in tempo utile un parere sui riscontri della Commissione europea, individuando eventuali carenze nel quadro giuridico in materia di adeguatezza e formulando eventuali raccomandazioni ove necessario.

17. A norma dell'articolo 36, paragrafo 4, della LED, spetta alla Commissione europea controllare su base continuativa gli sviluppi che potrebbero incidere sul funzionamento delle decisioni di adeguatezza.

18. L'articolo 36, paragrafo 3, della LED stabilisce che deve essere effettuato un riesame periodico almeno ogni quattro anni. Si tratta di un'indicazione temporale generica, che deve essere adattata a ciascun paese terzo o a ciascuna

organizzazione internazionale tramite una decisione di adeguatezza. A seconda delle circostanze particolari del caso, potrebbe essere giustificata una frequenza più breve. Inoltre, un incidente o nuove informazioni sul quadro giuridico del paese terzo o dell'organizzazione internazionale o una modifica dello stesso potrebbero rendere necessario anticipare il riesame rispetto al previsto. Sarebbe inoltre opportuno procedere tempestivamente a un primo riesame di una decisione di adeguatezza interamente nuova e adattare progressivamente il ciclo di riesame in base all'esito di tale attività.

19. Alla luce del compito del comitato di fornire alla Commissione un parere per valutare se il paese terzo, il territorio o uno o più settori specifici all'interno di tale paese terzo, o l'organizzazione internazionale non assicurino più un livello adeguato di protezione, il comitato deve ricevere a tempo debito dalla Commissione europea informazioni significative sul monitoraggio degli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale in questione. Il comitato dovrebbe quindi essere tenuto informato su eventuali processi di riesame e missioni di valutazione in corso nel paese terzo o con riferimento all'organizzazione internazionale. Il comitato raccomanda di essere invitato a partecipare a tali processi di riesame e missioni, come previsto nella decisione sullo scudo per la privacy e nella decisione di adeguatezza relativa al Giappone.

20. Va inoltre rilevato che, a norma dell'articolo 36, paragrafo 5, della LED, la Commissione europea ha la facoltà di revocare, modificare o sospendere le decisioni di adeguatezza in vigore nel caso in cui il paese terzo o l'organizzazione internazionale non garantisca più un livello di protezione adeguato. La procedura di revoca, modifica o sospensione coinvolge il comitato, chiamato a esprimere il suo parere in merito conformemente all'articolo 51, paragrafo 1, lettera g), della LED.

21. Inoltre, fatti salvi i poteri delle autorità preposte all'esercizio dell'azione penale, le autorità di controllo dovrebbero inoltre avere la facoltà di agire in sede giudiziale o stragiudiziale in caso di violazione della LED[13]. Dalla sentenza Schrems I della Corte di giustizia dell'Unione europea si desume in particolare che le autorità di protezione dei dati devono essere in grado di avviare procedimenti giudiziari dinanzi gli organi giurisdizionali nazionali qualora ritengano che un reclamo promosso da una persona nei confronti di una decisione di adeguatezza sia ben fondato[14]. La sentenza *Schrems II* ha confermato tale valutazione[15].

4. NORME UE CONCERNENTI L'ADEGUATEZZA NELLA COOPERAZIONE DI POLIZIA E NELLA COOPERAZIONE GIUDIZIARIA IN MATERIA PENALE

22. Nel merito le decisioni di adeguatezza dovrebbero concentrarsi sulla valutazione della legislazione vigente nel paese terzo interessato nel suo complesso, a livello teorico e pratico, alla luce dei criteri di valutazione di cui all'articolo 36 della LED. Il sistema di un paese terzo o di un'organizzazione internazionale deve prevedere i meccanismi e i principi generali fondamen-

tali di procedura e applicazione della legislazione in materia di protezione dei dati di cui in appresso.

23. L'articolo 36, paragrafo 2, della LED stabilisce gli elementi che la Commissione europea deve prendere in considerazione nel valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale.

24. In particolare, la Commissione deve prendere in considerazione lo Stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali[16], la legislazione pertinente, l'attuazione di tale legislazione, l'esistenza di diritti effettivi ed azionabili degli interessati e di un mezzo di ricorso effettivo in sede amministrativa e giudiziale per gli interessati i cui personali vengono trasferiti, l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti e gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale.

25. È chiaro dunque che qualsiasi analisi significativa dell'adeguatezza della protezione deve comprendere due elementi fondamentali: il contenuto delle norme applicabili e i mezzi per garantirne l'effettiva attuazione nella pratica. Spetta alla Commissione europea verificare sistematicamente che le norme in vigore siano efficaci nella pratica.

26. Il "nucleo" dei principi generali in materia di protezione dei dati e delle prescrizioni di "procedura e applicazione", la cui osservanza potrebbe essere considerata una condizione minima di adeguatezza della protezione, è tratto dalla Carta dei diritti fondamentali dell'Unione europea (la Carta) e dalla LED. Le disposizioni generali sulla protezione dei dati e la vita privata nel paese terzo non sono sufficienti. Nel quadro giuridico del paese terzo o dell'organizzazione internazionale devono figurare anche disposizioni specifiche che assicurino concretamente il diritto alla protezione dei dati nel settore delle attività di contrasto. Il paese terzo dovrebbe offrire garanzie atte ad assicurare un livello di protezione adeguato, sostanzialmente equivalente a quello garantito all'interno dell'Unione. Tali disposizioni devono essere azionabili.

27. Inoltre, per quanto concerne il principio della proporzionalità[17], in relazione alle leggi degli Stati membri, la Corte di giustizia dell'Unione europea ha ritenuto che la questione relativa al fatto che una limitazione dei diritti alla vita privata e alla protezione dei dati possa essere giustificata deve essere valutata, da un lato, misurando la **gravità dell'ingerenza** implicata da tale limitazione[18] e, dall'altro, verificando che l'**importanza dell'obiettivo di interesse pubblico** perseguito da tale limitazione sia proporzionato a tale gravità[19].

28. Secondo la giurisprudenza della Corte di giustizia dell'Unione europea, per soddisfare il principio di proporzionalità, una base giuridica che consente ingerenze nei diritti fondamentali deve definire essa stessa la portata della limitazione dell'esercizio del diritto di cui trattasi e prevedere norme chiare e precise che regolino la portata e l'applicazione della misura[20]. Deroghe alla protezione dei dati personali devono operare nei limiti dello stretto necessario[21]. Al fine di soddisfare tale prescrizione, oltre a stabilire norme chiare e precise che regolino la portata e l'applicazione della misura in questione, la normativa interessata deve imporre misure di salvaguardia minime, in modo

che le persone i cui dati sono trasferiti dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi. "In particolare, essa deve indicare in quali circostanze e a quali condizioni possa essere adottata una misura che prevede il trattamento di siffatti dati, garantendo così che l'ingerenza sia limitata allo stretto necessario. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatizzato"[22].

29. Il comitato ha adottato raccomandazioni che individuano garanzie essenziali, che riflettono la giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo (Corte EDU) nel settore della sorveglianza, che devono essere riscontrate nel diritto del paese terzo quando si valutano le ingerenze di tali misure di sorveglianza del paese terzo rispetto ai diritti degli interessati nel caso in cui i dati siano trasferiti in tale paese ai sensi del regolamento generale sulla protezione dei dati[23]. Ai fini della valutazione del rispetto delle condizioni di cui all'articolo 36, paragrafo 2, lettera a), della LED, il comitato ritiene che le garanzie stabilite nelle presenti raccomandazioni debbano essere prese in considerazione nel momento in cui si valuta l'adeguatezza di un paese terzo nel quadro di tale direttiva nel settore della sorveglianza, tenendo presenti ulteriori condizioni specifiche in detto settore in questo contesto.

30. In relazione alla prescrizione di cui all'articolo 36, paragrafo 2, lettera b), il paese terzo dovrebbe assicurare non soltanto un effettivo controllo indipendente della protezione dei dati, ma prevedere anche meccanismi di cooperazione con le autorità di protezione dei dati degli Stati membri[24].

31. In relazione alla prescrizione di cui all'articolo 36, paragrafo 2, lettera c), al di là degli impegni internazionali che il paese terzo o l'organizzazione internazionale ha assunto, si dovrebbero tenere altresì in considerazione gli obblighi derivanti dalla partecipazione del paese terzo o dell'organizzazione internazionale a sistemi multilaterali o regionali, in particolare rispetto alla protezione dei dati personali, nonché l'attuazione di tali obblighi, in particolare l'adesione del paese terzo ad altri accordi internazionali in materia di protezione dei dati, ad esempio la convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale e relativo protocollo addizionale (convenzione 108[25] e la sua versione modernizzata, convenzione 108+). Si può tenere conto anche del rispetto da parte del paese del terzo paese dei principi sanciti in documenti internazionali quali il documento del Consiglio d'Europa *Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime*.

32. Una decisione di adeguatezza dovrebbe garantire che, attraverso il contenuto dei diritti in materia di vita privata e protezione dei dati e la loro attuazione, vigilanza e applicazione efficaci, il sistema del paese terzo nel suo complesso garantisca il livello di protezione richiesto, anche per i dati in transito verso tale paese terzo. Come sottolineato dalla Corte di giustizia dell'Unione europea nella sentenza *Schrems II*, il livello elevato di protezione offerto dovrebbe essere garantito altresì durante il trasferimento dei dati verso un paese terzo[26].

33. Infine, nell'adottare una decisione di adeguatezza nei confronti di un territorio o di un settore specifico all'interno di un paese terzo, la Commissione europea dovrebbe prendere in considerazione criteri chiari e obiettivi come specifiche attività di trattamento o l'ambito di applicazione delle norme giuridiche e degli atti legislativi applicabili in vigore nel paese terzo[27].

A. PRINCIPI GENERALI E GARANZIE

a) Nozioni

34. Dovrebbero esservi nozioni basilari in materia di protezione dei dati. Tali nozioni non devono necessariamente riprendere la terminologia della LED, ma dovrebbero rispecchiare ed essere coerenti con le nozioni sancite nel diritto europeo in materia di protezione dei dati. A titolo esemplificativo, la LED contiene le seguenti nozioni fondamentali: "dati personali", "trattamento dei dati personali", "autorità competente", "titolare del trattamento", "responsabile del trattamento", "destinatario", "dati sensibili", "esattezza", "profilazione", "protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita", "autorità di controllo" e "pseudonimizzazione".

b) Liceità e correttezza del trattamento dei dati personali
(articolo 4 - considerando 26)

35. Ai sensi dell'articolo 8, paragrafo 2, della Carta, i dati personali dovrebbero tra l'altro essere trattati "per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge"[28]. Tuttavia, nel contesto delle attività di contrasto, occorre rilevare che l'adempimento dei compiti di prevenzione, indagine, accertamento e perseguimento di reati, affidato istituzionalmente dalla legge alle autorità competenti, consente a queste ultime di richiedere od ordinare alle persone fisiche di dare seguito alle richieste formulate. In tal caso il consenso dell'interessato non dovrebbe costituire la base giuridica per il trattamento dei dati personali da parte delle autorità competenti[29].
36. Tale base giuridica dovrebbe stabilire norme chiare e precise che disciplinano la portata e l'applicazione delle attività di trattamento dei dati pertinenti e imporre misure di salvaguardia minime[30]. Inoltre la Corte di giustizia dell'Unione europea ha ricordato che tale "normativa dev'essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale"[31].
37. Per essere lecito, il trattamento dei dati[32] dovrebbe essere necessario per l'esecuzione di un compito svolto da un'autorità competente ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, comprese le misure di salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica[33]. Tali finalità dovrebbero essere previste dal diritto nazionale.
38. I dati personali devono essere trattati correttamente. Il principio di trattamento corretto proprio della protezione dei dati è una nozione distinta dal

diritto a un giudice imparziale sancito dall'articolo 47 della Carta e nell'articolo 6 della convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU)[34].

c) Il principio della limitazione delle finalità (articolo 4)

39. Le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta[35].

40. I dati dovrebbero essere trattati per una finalità determinata, esplicita e legittima a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali[36], incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica nel paese terzo, e successivamente utilizzati per uno qualsiasi di tali fini nella misura in cui ciò non sia incompatibile con la finalità originale del trattamento (ad esempio per procedimenti di esecuzione paralleli o a fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici) e sia soggetto a garanzie adeguate per i diritti e le libertà degli interessati. Se i dati personali sono trattati dallo stesso o da un altro titolare del trattamento (autorità competente[37]) per una finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali diversa da quella per la quale sono stati raccolti, tale trattamento dovrebbe essere consentito purché sia autorizzato conformemente alle disposizioni giuridiche applicabili e sia necessario e proporzionato a tale altra finalità[38]. Dovrebbe essere presa in considerazione l'esistenza di un meccanismo per informare le autorità competenti degli Stati membri pertinenti in merito a tale ulteriore trattamento dei dati[39]. Inoltre in ogni caso il livello di protezione delle persone fisiche previsto nell'Unione dalla LED non dovrebbe essere compromesso, anche nei casi di trasferimenti dei dati personali dal paese terzo verso titolari del trattamento o responsabili del trattamento nello stesso paese terzo[40].

d) Condizioni specifiche per l'ulteriore trattamento per finalità diverse (articolo 9)

41. Per quanto riguarda l'ulteriore trattamento o la divulgazione di dati trasferiti dall'UE per finalità diverse da quelle di contrasto, quali quelle relative alla sicurezza nazionale, la legge dovrebbe altresì prevedere che esse siano necessarie e proporzionate. Dovrebbe essere presa in considerazione l'esistenza di un meccanismo per informare le autorità competenti degli Stati membri pertinenti in merito a tale ulteriore trattamento dei dati[41]. Anche in questo caso, una volta ulteriormente trattati o divulgati, i dati dovrebbero beneficiare del medesimo livello di protezione di cui godevano nel momento in cui sono stati trattati inizialmente dall'autorità competente ricevente.

e) Il principio della minimizzazione dei dati

42. I dati dovrebbero essere adeguati, pertinenti e non eccedenti rispetto alle finalità perseguite. In particolare occorre prendere in considerazione l'applicazione dei requisiti relativi alla protezione dei dati fin dalla progettazione

e alla protezione per impostazione predefinita, quali campi di inserimenti limitati (comunicazioni strutturate) o controlli della qualità automatizzati e non automatizzati.

f) Il principio dell'esattezza dei dati

43. I dati dovrebbero essere esatti e, se necessario, aggiornati. Tuttavia il principio dell'esattezza dei dati dovrebbe essere applicato tenendo conto della natura e della finalità del trattamento in questione. In particolare nei procedimenti giudiziari, le dichiarazioni contenenti dati personali sono basate sulla percezione soggettiva delle persone e non sempre sono verificabili. Il requisito dell'esattezza non dovrebbe pertanto riferirsi all'esattezza di una dichiarazione ma al semplice fatto che è stata rilasciata[42].

44. Si dovrebbe garantire che i dati personali inesatti, incompleti o non più aggiornati non siano trasmessi o resi disponibili[43] e che siano previste procedure per correggere o eliminare dati imprecisi. In particolare si dovrebbe prendere in considerazione qualsiasi sistema di classificazione delle informazioni trattate, in termini di affidabilità della fonte e livello di verifica dei fatti[44].

g) Il principio della conservazione dei dati

45. I dati dovrebbero essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. Occorre istituire meccanismi adeguati per la cancellazione dei dati personali; può trattarsi di un periodo fisso o di un riesame periodico della necessità di conservazione dei dati personali (oppure una combinazione di entrambi: periodo massimo fisso e riesame periodico a determinati intervalli)[45]. I dati personali conservati per periodi più lunghi per fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici dovrebbero essere soggetti a garanzie adeguate (ad esempio in relazione all'accesso)[46].

h) Il principio della sicurezza e della riservatezza
(articolo 29, considerando 28 e 71)

46. Qualsiasi entità che tratti dati personali dovrebbe assicurare che essi siano trattati in modo da garantirne un'adeguata sicurezza per impedire l'accesso o l'utilizzo non autorizzati dei dati personali e delle attrezzature impiegate per il trattamento. Ciò comprende la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti illeciti e dalla perdita, dalla distruzione o dal danno accidentali, e la disponibilità di misure adeguate per farvi fronte. Nel determinare il livello di sicurezza, occorre tenere conto dello stato dell'arte, dei costi di attuazione e della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi sventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

47. Occorre garantire canali sicuri di comunicazione tra le autorità degli Stati membri che trasferiscono i dati personali e le autorità riceventi dei paesi terzi.

i) Il principio della trasparenza
(articolo 13; considerando 26, 39, 42, 43, 44, 46)

48. È opportuno che le persone fisiche siano sensibilizzate rispetto ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento dei loro dati personali, nonché alle modalità di esercizio dei loro diritti in relazione al trattamento[47].

49. Dovrebbero essere messe a disposizione delle persone fisiche informazioni su tutti i principali elementi del trattamento dei loro dati personali. Tali informazioni dovrebbero essere facilmente accessibili e di facile comprensione ed essere scritte in un linguaggio semplice e chiaro. Tali informazioni dovrebbero comprendere la finalità del trattamento, l'identità del titolare del trattamento, i diritti di cui gode l'interessato[48] e altre informazioni nella misura in cui ciò sia necessario a garantire la correttezza.

50. Possono esistere alcune eccezioni a tale diritto di informazione. Tale limitazione dovrebbe tuttavia essere consentita da una misura legislativa ed essere necessaria e proporzionata per non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari, per non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, per proteggere la sicurezza pubblica o la sicurezza nazionale o per tutelare i diritti e le libertà altrui, per il tempo in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata. Tali limitazioni dovrebbero altresì essere prese in considerazione e valutate tenendo conto della possibilità di proporre reclamo a un'autorità di controllo o di proporre ricorso giurisdizionale. In ogni caso, qualsiasi eventuale limitazione dovrebbe essere temporanea e non generalizzata e dovrebbe essere inquadrata da condizioni, garanzie e limitazioni analoghe a quelle previste dalla Carta e dalla CEDU, come interpretate rispettivamente nella giurisprudenza della Corte di giustizia dell'Unione europea e dalla Corte EDU, e rispettare in particolare la sostanza di tali diritti e libertà.

j) Il diritto di accesso, rettifica e cancellazione (articoli 14 e 16)

51. L'interessato dovrebbe avere il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati che lo riguardano e, in tal caso, di ottenere l'accesso ai propri dati. Tale diritto dovrebbe comprendere quanto meno determinate informazioni in merito al trattamento, quali le finalità e la base giuridica per il trattamento, il diritto di proporre reclamo presso l'autorità di controllo o le categorie di dati personali in questione[49]. Ciò è particolarmente importante nel caso in cui la trasparenza sia conseguita mediante una notifica generale (ad esempio informazioni sul sito web dell'autorità).

52. L'interessato dovrebbe avere il diritto di ottenere la rettifica dei propri dati per motivi specifici, ad esempio qualora risultino essere inesatti o incompleti. L'interessato dovrebbe inoltre avere il diritto di ottenere la cancellazione

dei propri dati quando, ad esempio, il loro trattamento non è più necessario o è illecito.

53. L'esercizio di tali diritti non dovrebbe essere eccessivamente oneroso per l'interessato.

k) Limitazioni dei diritti degli interessati

54. Possibili limitazioni a tali diritti potrebbero sussistere per non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari, per non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, per proteggere la sicurezza pubblica o la sicurezza nazionale o per tutelare i diritti e le libertà altrui, per il tempo in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata. Tali limitazioni dovrebbero altresì essere prese in considerazione e valutate tenendo conto della possibilità di proporre reclamo a un'autorità di controllo o di proporre ricorso giurisdizionale.

l) Limitazione relativa ai trasferimenti successivi
(articolo 35, considerando 64 e 65)

55. I trasferimenti successivi di dati personali da parte del destinatario iniziale verso un altro paese terzo o un'altra organizzazione internazionale non devono compromettere il livello di protezione, previsto nell'Unione, delle persone fisiche i cui dati vengono trasferiti. Di conseguenza tali trasferimenti successivi di dati dovrebbero essere consentiti soltanto laddove sia garantita la continuità del livello di protezione offerto dal diritto dell'Unione[50]. In particolare il destinatario successivo (ossia il destinatario del trasferimento successivo) dovrebbe essere un'autorità competente per fini di contrasto[51] e tali trasferimenti successivi possono avvenire soltanto per finalità limitate e determinate e purché vi sia una base giuridica per tale trattamento.

56. Dovrebbe essere presa in considerazione anche l'esistenza di un meccanismo che consenta alle autorità competenti dello Stato membro interessato di essere informate e di autorizzare un tale trasferimento successivo dei dati. Il destinatario iniziale dei dati trasferiti dall'UE dovrebbe essere responsabile ed essere in grado di dimostrare che l'autorità competente pertinente dello Stato membro ha autorizzato il trasferimento successivo[52] e che sono previste garanzie adeguate per i trasferimenti successivi in assenza di una decisione di adeguatezza relativa al paese terzo verso il quale i dati verrebbero ulteriormente trasferiti[53].

m) Principio di responsabilizzazione (articolo 4, paragrafo 4)

57. Il titolare del trattamento dovrebbe essere responsabile ed essere in grado di dimostrare il rispetto dei principi di protezione dei dati di cui all'articolo 4 della LED.

B. ESEMPI DI PRINCIPI SUPPLEMENTARI DA APPLICARE A TIPI SPECIFICI DI TRATTAMENTO

a) Categorie particolari di dati (articolo 10 e considerando 37)

58. Nel caso in cui siano interessate "categorie particolari di dati"[54] dovrebbero esistere garanzie specifiche destinate ad affrontare i rischi specifici in questione[55]. Tali categorie dovrebbero riflettere quelle previste all'articolo 10 della LED. Il trattamento di categorie particolari di dati dovrebbe pertanto essere soggetto a garanzie specifiche ed essere consentito soltanto se strettamente necessario a determinate condizioni, ad esempio per tutelare gli interessi vitali di una persona.

b) Processo decisionale automatizzato e profilazione
(articolo 11 e considerando 38)

59. Le decisioni basate unicamente sul trattamento automatizzato (processo decisionale automatizzato relativo alle persone fisiche), compresa la profilazione, che producono effetti giuridici negativi che riguardano l'interessato o incidono significativamente sulla sua persona dovrebbero avvenire soltanto a determinate condizioni stabilite dal quadro giuridico del paese terzo[56].
60. Nel quadro dell'Unione europea, tali condizioni comprendono ad esempio il rilascio di specifiche informazioni all'interessato e il diritto di ottenere l'intervento umano presso il titolare del trattamento, in particolare il diritto di esprimere la propria opinione, di ottenere una spiegazione della decisione raggiunta dopo tale valutazione e di impugnare la decisione.
61. Il diritto del paese terzo dovrebbe, in ogni caso, prevedere le garanzie necessarie per i diritti e le libertà dell'interessato. A tale riguardo dovrebbe essere presa in considerazione l'esistenza di un meccanismo per informare le autorità competenti dello Stato membro pertinente in merito a qualsiasi ulteriore trattamento, come l'uso dei dati trasferiti per la profilazione su larga scala.

c) Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (articolo 20)

62. Nel valutare l'adeguatezza, l'attenzione dovrebbe essere rivolta all'esistenza di un obbligo in capo ai titolari del trattamento di adottare politiche interne e attuare misure che aderiscono ai principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, al fine di adottare misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie.

C. MECCANISMI DI PROCEDURA E APPLICAZIONE

63. Anche se gli strumenti dei quali il paese terzo si avvale per assicurare un livello di protezione adeguato possono essere diversi da quelli attuati all'interno dell'Unione europea[57], un sistema coerente con quello europeo deve essere caratterizzato dalla presenza degli elementi di cui in appresso.

a) Autorità di controllo indipendente competente (articolo 36, paragrafo 2, lettera b), articolo 36, paragrafo 3 e considerando 67)

64. Dovrebbero essere presenti una o più autorità di controllo indipendenti, aventi il compito di garantire e far rispettare le disposizioni in materia di protezione dei dati e della vita privata. L'autorità di controllo agisce in piena indipendenza e imparzialità nell'adempimento dei suoi compiti e nell'esercizio dei suoi poteri, senza richiedere né accettare istruzioni. In tale contesto, l'autorità di controllo dovrebbe disporre di tutti i poteri di esecuzione per garantire in maniera efficace la conformità ai diritti in materia di protezione dei dati e per sensibilizzare l'opinione pubblica al riguardo. Dovrebbero inoltre essere presi in considerazione il personale e il bilancio dell'autorità di controllo. L'autorità di controllo dovrebbe essere in grado, infine, di condurre indagini di propria iniziativa. Dovrebbe inoltre essere incaricata di assistere e consigliare gli interessati nell'esercizio dei loro diritti (cfr. anche la seguente lettera c)). Le decisioni di adeguatezza dovrebbero individuare, se del caso, la o le autorità di controllo e i meccanismi di cooperazione con le autorità di controllo degli Stati membri per far rispettare le norme in materia di protezione dei dati.

b) Attuazione efficace delle norme in materia di protezione dei dati

65. Il sistema di un paese terzo dovrebbe garantire che i titolari del trattamento e chi tratta per conto loro i dati personali abbiano un buon livello di consapevolezza dei propri obblighi, compiti e responsabilità, e che gli interessati siano consapevoli dei propri diritti e dei mezzi a disposizione per esercitarli. L'esistenza di sanzioni effettive e dissuasive può svolgere un ruolo importante nel garantire il rispetto delle norme, così come la presenza di sistemi di verifica diretta da parte di autorità, ispettori o addetti indipendenti alla protezione dei dati.

66. Il quadro per la protezione dei dati di un paese terzo dovrebbe obbligare i titolari del trattamento o i soggetti che trattano i dati personali per loro conto a rispettarne le disposizioni e a fornire le prove di tale conformità, in particolare all'autorità di controllo competente. Tali misure dovrebbero comprendere la conservazione di registri o fascicoli di registrazione delle attività di trattamento dei dati per un periodo di tempo adeguato. Possono comprendere anche, ad esempio, valutazioni d'impatto sulla protezione dei dati, la designazione di un responsabile della protezione dei dati o la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita.

c) il sistema di protezione dei dati deve facilitare l'esercizio dei diritti dell'interessato (articoli 12, 17 e 46 della LED)

67. Il quadro di protezione dei dati di un paese terzo dovrebbe obbligare i titolari del trattamento dei dati a facilitare l'esercizio dei diritti degli interessati di cui alla precedente sezione A, lettera j) e prevedere che l'autorità di vigilanza, su richiesta, informi qualsiasi interessato in merito all'esercizio dei suoi diritti[58].

d) Il sistema di protezione dei dati deve prevedere meccanismi di ricorso adeguati

68. Sebbene attualmente non esista una giurisprudenza relativa all'adeguatezza dell'ordinamento giuridico di un paese terzo ai sensi della LED, la Corte di giustizia dell'Unione europea ha interpretato il diritto fondamentale a una tutela giurisdizionale effettiva sancito dall'articolo 47 della Carta. L'articolo 47, primo comma, della Carta stabilisce che ogni individuo i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice[59], nel rispetto delle condizioni previste da tale articolo.

69. Secondo una giurisprudenza costante della Corte di giustizia dell'Unione europea, l'esistenza stessa di un controllo giurisdizionale effettivo volto a garantire il rispetto delle disposizioni del diritto dell'Unione è inerente all'esistenza dello Stato di diritto. Di conseguenza la legislazione che non prevede alcuna possibilità per una persona fisica di disporre di mezzi di ricorso per avere accesso ai dati personali che la riguardano, o di ottenere la rettifica o la cancellazione di tali dati, non rispetta l'essenza del diritto fondamentale a una tutela giurisdizionale effettiva, come sancito all'articolo 47 della Carta[60].

70. L'interessato dovrebbe essere in grado di avvalersi di mezzi di ricorso per far valere i propri diritti con rapidità ed efficacia, e senza costi proibitivi, nonché per garantire la conformità.

71. A tal fine devono essere disponibili meccanismi di controllo che consentano un'indagine indipendente sulle denunce e che permettano di individuare e sanzionare nella pratica eventuali violazioni del diritto alla protezione dei dati e al rispetto della vita privata.

72. In caso di inosservanza delle norme, all'interessato i cui dati sono stati trasferiti verso il paese terzo dovrebbe inoltre essere riconosciuto un mezzo di ricorso effettivo in sede amministrativa e giudiziale nel paese terzo, anche ai fini del risarcimento per i danni subiti a causa di un trattamento illecito dei dati personali che lo riguardano. Si tratta di un elemento fondamentale che deve prevedere un sistema di conciliazione indipendente o di arbitrato che permetta l'eventuale pagamento di indennizzi o l'imposizione di sanzioni.

NOTE

[1] GU L 119 del 4.5.2016, pag. 89.

[2] WP254 rev.01, adottato dal gruppo di lavoro Articolo 29 il 28 novembre 2017, versione emendata e adottata il 6 febbraio 2018, che aggiorna il capitolo I del documento di lavoro "Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati", WP12, adottato dal gruppo di lavoro Articolo 29 il 24 luglio 1998.

[3] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati (GU L 119 del 4.5.2016, pag. 1).

[4] Causa C-311/18, Data Protection Commissioner/Facebook Ireland Limited e Maximillian Schrems, 16 luglio 2020, ECLI:EU:C:2020:559, punto 92 (Schrems II).

[5] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

[6] Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (GU L 350 del 30.12.2008, pag. 60).

[7] Causa C362/14, Maximillian Schrems/Data Protection Commissioner, 6 ottobre 2015, ECLI:EU:C:2015:650, punti 73 e 74 (Schrems I).

[8] *Schrems I*, punto 88.

[9] Articolo 288 del TFUE.

[10] *Schrems I*, punto 52.

[11] Considerando 67 della LED.

[12] *Schrems I*, punti da 72 a 74 e parere 1/15 della Corte di giustizia dell'Unione europea del 26 luglio 2017 sul progetto di accordo tra il Canada e l'Unione europea, ECLI:EU:C:2017:592 (parere 1/15), punto 134: "[t]ale diritto alla protezione dei dati di carattere personale richiede, in particolare, che la continuità del livello elevato di protezione delle libertà e dei diritti fondamentali riconosciuti dal diritto dell'Unione sia garantita in caso di trasferimento di dati personali dall'Unione a un paese terzo. Anche se le misure dirette ad assicurare un siffatto livello di protezione possono essere diverse da quelle attuate all'interno dell'Unione al fine di garantire il rispetto degli obblighi risultanti dal diritto dell'Unione, tali misure devono cionondimeno rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione".

[13] Cfr. articolo 47, paragrafo 5 e considerando 82 della LED.

[14] Cfr. *Schrems I*, punto 65: "[...] incombe al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all'esame della validità di tale decisione".

[15] Cfr. *Schrems II*, punto 120: "anche in presenza di una decisione di adeguatezza della Commissione, l'autorità nazionale di controllo competente, investita da una persona di un reclamo relativo alla protezione dei suoi diritti e delle sue libertà rispetto ad un trattamento di dati personali che la riguardano, deve poter esaminare, in piena indipendenza, se il trasferimento di tali dati rispetti i requisiti posti dal RGPD e, se del caso, proporre un ricorso dinanzi ai giudici nazionali affinché questi ultimi procedano, se condividono i dubbi di tale autorità quanto alla validità della decisione di adeguatezza, ad un rinvio pregiudiziale diretto all'esame della suddetta validità".

[16] Nel valutare il quadro giuridico del paese terzo, occorre tenere conto della possibilità che si possa giungere all'imposizione della pena di morte o di qualsiasi forma di trattamento crudele e inumano sulla base dei dati trasferiti dall'UE. In effetti, qualora tale pena o trattamento sia previsto nel diritto del paese terzo, occorre trovare misure di salvaguardia ulteriori nel quadro giuridico del paese terzo atte a garantire che i dati trasferiti dall'UE non vengano utilizzati per richiedere, pronunciare o eseguire una pena di morte o qualsiasi forma di trattamento crudele e inumano (ad esempio un accordo internazionale che impone condizioni sul trasferimento, un impegno da parte del paese terzo a non imporre una

pena di morte o qualsiasi forma di trattamento crudele e inumano sulla base di dati trasferiti dall'UE oppure una moratoria in merito alla pena di morte).

[17] Articolo 52, paragrafo 1, della Carta.

[18] La Corte ha rilevato ad esempio che "l'ingerenza derivante dalla raccolta in tempo reale dei dati che consentono di localizzare un'apparecchiatura terminale risulta particolarmente grave, dato che tali dati forniscono alle autorità nazionali competenti uno strumento di controllo preciso e permanente degli spostamenti degli utenti dei telefoni mobili [...]" (cause riunite C-511/18, C-512/18 e C-520/18, La Quadrature du Net e a., 6 ottobre 2020, ECLI:EU:C:2020:791, punto 187, compresa la giurisprudenza ivi citata).

[19] *La Quadrature du Net e a.*, punto 131.

[20] *Schrems II*, punto 180.

[21] *Schrems II*, punto 176, compresa la giurisprudenza citata.

[22] *Schrems II*, punto 176, compresa la giurisprudenza citata.

[23] Comitato europeo per la protezione dei dati, Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza, adottate il 10 novembre 2020.

[24] Considerando 67 della LED.

[25] Considerando 68 della LED.

[26] Cfr. punto 93.

[27] Considerando 67 della LED.

[28] Cfr. *Schrems II*, punto 173.

[29] Il considerando 35 della LED afferma inoltre che "[q]ualora sia tenuto ad adempiere un obbligo legale, l'interessato non è in grado di operare una scelta autenticamente libera, pertanto la sua reazione non potrebbe essere considerata una manifestazione di volontà libera. Ciò non dovrebbe impedire agli Stati membri di prevedere per legge che l'interessato possa acconsentire al trattamento dei propri dati personali ai fini della presente direttiva, ad esempio per test del DNA nell'ambito di indagini penali o per il monitoraggio della sua ubicazione mediante dispositivo elettronico per l'esecuzione di sanzioni penali".

[30] Cfr. Schrems II, punti 175 e 180 e parere 1/15, punto 139 e la giurisprudenza citata.

[31] Cfr. causa C-623/17, Privacy International/Secretary of State for Foreign and Commonwealth Affairs e a., 6 ottobre 2020, ECLI:EU:C:2020:790, punto 68 - Dovrebbe inoltre essere chiaro che nella versione francese della sentenza, la Corte utilizza la parola "réglementation" che è più ampia rispetto ai soli atti del Parlamento.

[32] Il trattamento interamente o parzialmente automatizzato di dati personali e il trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

[33] Le autorità competenti sono un'autorità pubblica competente per tali finalità o qualsiasi altro organismo o entità incaricato/a dalla legge ad esercitare poteri pubblici a tali fini.

[34] Considerando 26 della LED.

[35] Considerando 26 della LED.

[36] Comprese "le attività di polizia condotte senza previa conoscenza della rilevanza penale di un fatto. Tali attività possono comprendere anche l'esercizio di poteri mediante l'adozione di misure coercitive quali le attività di polizia in occasione di manifestazioni, grandi eventi sportivi e sommosse. Esse comprendono anche il mantenimento dell'ordine pubblico quale compito conferito alla polizia o ad altre autorità incaricate dell'applicazione della legge ove necessario per la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica e agli interessi fondamentali della società tutelati dalla legge che possono dar luogo a reati" (considerando 12 della LED). Occorre operare una distinzione rispetto alla finalità della sicurezza nazionale o alle attività rientranti nell'ambito di applicazione del titolo V, capo 2, del trattato sull'Unione europea (TUE) (considerando 14 della LED).

[37] Cfr. nota 33.

[38] Considerando 29 della LED.

[39] Tale meccanismo potrebbe essere ad esempio il ricorso a codici di gestione concordati di comune accordo, un obbligo di notifica nel quadro di uno strumento internazionale, comprese possibili notifiche automatizzate o altre misure di trasparenza analoghe.

[40] Considerando 64 della LED.

[41] Cfr. nota 39.

[42] Considerando 30 della LED.

[43] Considerando 32 della LED.

[44] Ad esempio griglie 4x4 per valutazioni dell'affidabilità e codici di gestione.

[45] Articolo 5 della LED.

[46] Considerando 26 della LED.

[47] Considerando 26 della LED.

[48] Tanto i diritti sostanziali (diritto di accesso, di rettifica, ecc.) quanto il diritto di ricorso.

[49] Articolo 14 della LED.

[50] Cfr. anche parere 1/15.

[51] Cfr. nota 33.

[52] In tale contesto è opportuno prendere in considerazione l'esistenza di un obbligo o un impegno ad attuare codici di gestione pertinenti definiti dalle autorità dello Stato membro che effettua il trasferimento.

[53] I requisiti di cui sopra non pregiudicano le condizioni specifiche per i trasferimenti successivi verso un paese adeguato stabilite nel quadro della LED (articolo 35, paragrafo 1, lettere c) ed e)).

[54] Tali categorie particolari sono anche qualificate dati "sensibili" al considerando 37 della LED.

[55] Tali garanzie aggiuntive potrebbero essere ad esempio misure specifiche di sicurezza, diritti di accesso limitato per il personale, limitazioni relative all'ulteriore trattamento, processo decisionale automatizzato, condivisione successiva o trasferimenti successivi.

[56] Parere 1/15, punto 173.

[57] Schrems I, punto 74.

[58] L'esercizio dei diritti degli interessati potrebbe essere diretto o indiretto.

[59] La Corte di giustizia dell'Unione europea ritiene che una tutela giurisdizionale effettiva possa essere garantita non soltanto da un organo giurisdizionale, ma anche da un organo che offre garanzie sostanzialmente equivalenti a quelle richieste dall'articolo 47 della Carta (cfr. Schrems II, punto 197). Ciò potrebbe interessare in particolare le organizzazioni internazionali.

[60] Schrems II, punti 187 e 194, compresa la giurisprudenza citata.

Dichiarazione in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – *Data Protection Commissioner contro Facebook Ireland e Maximillian Schrems*

adottata il 17 luglio 2020

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI (EDPB) HA ADOTTATO LA SEGUENTE DICHIARAZIONE.

L'EDPB accoglie con favore la sentenza della CGUE, che sottolinea il diritto fondamentale alla privacy nel quadro del trasferimento di dati personali verso paesi terzi. La decisione della CGUE riveste grande importanza. L'EDPB ha preso atto del fatto che la Corte di giustizia invalida la decisione 2016/1250 sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy e considera valida la decisione della Commissione 2010/87 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a responsabili del trattamento stabiliti in paesi terzi.

L'EDPB ha discusso della sentenza della Corte nel corso della sua 34a sessione plenaria tenutasi il 17 luglio 2020.

Per quanto riguarda lo **scudo per la privacy**, l'EDPB sottolinea che l'UE e gli Stati Uniti dovrebbero creare un quadro esaustivo ed efficace che garantisca un livello di protezione dei dati personali negli Stati Uniti sostanzialmente equivalente a quello garantito nell'UE, in linea con la sentenza.

In passato l'EDPB aveva già individuato alcune delle principali carenze dello scudo per la privacy, sulle quali si basa la decisione della CGUE di dichiararlo invalido.

Nelle sue relazioni sulle revisioni annuali congiunte dello scudo per la privacy, l'EDPB ha messo in dubbio il rispetto dei principi di necessità e proporzionalità in materia di protezione dei dati nell'applicazione della normativa statunitense [1].

L'EDPB intende continuare a svolgere un ruolo costruttivo nel garantire un trasferimento transatlantico dei dati personali che apporti benefici ai cittadini e alle organizzazioni del SEE ed è pronto a fornire assistenza e orientamenti alla Commissione europea per contribuire a sviluppare, insieme agli Stati Uniti, un nuovo quadro che rispetti pienamente il diritto dell'UE in materia di protezione dei dati.

Se da una parte le **clausole contrattuali tipo (CCT)** rimangono valide, dall'altra la CGUE sottolinea la necessità di garantire che mantengano, all'atto pratico, un livello di protezione sostanzialmente equivalente a quello garantito dal RGPD alla luce della Carta dell'UE. È in primo luogo responsabilità dell'esportatore e dell'importatore, nel considerare l'opportunità di aderire alle CCT, valutare se i paesi verso i quali i dati vengono inviati conferiscano una protezione adeguata. Nell'effettuare tale valutazione preliminare, l'esportatore (se necessario con l'assistenza dell'importatore) tiene conto del contenuto delle CCT, delle circostanze specifiche del trasferimento e del regime giuridico applicabile nel paese dell'importatore. L'esame di quest'ultimo elemento è effettuato alla luce dei fattori non esaustivi di cui all'articolo 45, paragrafo 2, del RGPD.

Se tale valutazione giunge alla conclusione che il paese dell'importatore non conferisce un livello di protezione sostanzialmente equivalente, l'esportatore può dover prendere in considerazione l'introduzione di misure supplementari

rispetto a quelle previste dalle CCT. L'EDPB sta esaminando ulteriormente le misure supplementari che potrebbero essere adottate in questi casi.

La sentenza della CGUE sottolinea, inoltre, quanto sia importante che l'esportatore e l'importatore adempiano gli obblighi che incombono loro ai sensi delle CCT, in particolare quelli in materia di informazione relativamente a eventuali modifiche della normativa vigente nel paese dell'importatore. Quando tali obblighi contrattuali non sono o non possono essere adempiuti, l'esportatore è vincolato dalle CCT a sospendere il trasferimento o a denunciare le stesse CCT oppure ancora a notificare alla propria autorità di controllo competente se intende continuare a trasferire i dati.

L'EDPB prende atto del dovere delle autorità di controllo competenti di sospendere o vietare il trasferimento di dati verso un paese terzo basato sulle CCT qualora, a parere della competente autorità di controllo e alla luce di tutte le circostanze di detto trasferimento, tali clausole non siano o non possano essere rispettate nel suddetto paese terzo e la protezione dei dati trasferiti non possa essere garantita con altri mezzi, in particolare laddove il titolare o il responsabile del trattamento non abbiano già sospeso o annullato il trasferimento.

L'EDPB ricorda di avere pubblicato linee guida sulle deroghe di cui all'articolo 49 del RGPD [2], e che queste ultime devono essere applicate caso per caso.
L'EDPB valuterà più approfonditamente la sentenza e fornirà ulteriori chiarimenti alle parti interessate nonché orientamenti sull'uso degli strumenti per il trasferimento di dati personali verso paesi terzi a norma di tale sentenza.
L'EDPB e le autorità di controllo europee che lo compongono sono pronti, come dichiarato dalla CGUE, a garantire la coerenza in tutto il SEE.

Per il comitato europeo per la protezione dei dati
La presidente

(Andrea Jelinek)

NOTE

[1] Cfr. EDPB, EU-U.S. Privacy Shield - Second Annual Joint Review report (Scudo per la privacy UE-USA, seconda revisione annuale congiunta), https://edpb.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_en ed EDPB, EU -U.S. Privacy Shield - Third Annual Joint Review report (Scudo per la privacy UE-USA, terza revisione annuale congiunta), https://edpb.europa.eu /our-work-tools/our-documents/eu-us-privacy-shield-third-annual-joint-review-report-12112019_en

[2] Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento (UE) 2016/679, adottate il 25 maggio 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_it.pdf, pag. 3.

Domande più frequenti in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – *Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems*

adottate il 23 luglio 2020

Il presente documento intende offrire una risposta ad alcune delle domande più frequenti ricevute dalle autorità di controllo e sarà elaborato e integrato insieme a un'ulteriore analisi man mano che il comitato europeo per la protezione dei dati (EDPB) proseguirà nell'esame e nella valutazione della sentenza della Corte di giustizia dell'Unione europea (la "Corte").

La sentenza C-311/18 è consultabile qui, mentre il comunicato stampa della Corte è disponibile qui

1. Che cosa ha stabilito la Corte nella sentenza?

Nella sentenza la Corte ha esaminato la validità della decisione 2010/87/UE della Commissione europea, relativa alle clausole contrattuali tipo, e ha ritenuto la decisione valida. La validità di tale decisione non è infatti rimessa in discussione dal solo fatto che le clausole tipo di protezione dei dati di cui alla suddetta decisione, avendo natura contrattuale, non vincolano le autorità del paese terzo verso i quali i dati potrebbero essere trasferiti.

Per contro, la Corte ha precisato che tale validità dipende dall'esistenza all'interno della decisione 2010/87/UE di meccanismi efficaci che consentano, in pratica, di garantire il rispetto di un livello di protezione essenzialmente equivalente a quello garantito all'interno dell'UE dal RGPD e che prevedano la sospensione o il divieto dei trasferimenti di dati personali, fondati su tali clausole, in caso di violazione delle clausole stesse o in caso risulti impossibile garantirne l'osservanza.

A tale riguardo la Corte sottolinea, in particolare, che la decisione 2010/87/UE stabilisce l'obbligo per l'esportatore dei dati e il destinatario di tali dati (l'"importatore dei dati") di verificare, preliminarmente al trasferimento, e tenendo conto delle circostanze di quest'ultimo, se tale livello di protezione sia rispettato nel paese terzo considerato. Inoltre, la Corte rileva che la decisione 2010/87/UE impone all'importatore dei dati di informare l'esportatore di qualsiasi impossibilità di conformarsi alle clausole tipo di protezione nonché, ove necessario, a eventuali misure supplementari a quelle offerte dalle clausole, con l'onere, in tal caso, per l'esportatore dei dati di sospendere il trasferimento di dati e/o di risolvere il contratto concluso con l'importatore.

La Corte ha altresì esaminato la validità della decisione relativa allo «scudo per la privacy» (Decisione 2016/1250 sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy), poiché i trasferimenti in questione nel contesto della controversia nazionale sfociata nella domanda di pronuncia pregiudiziale hanno avuto luogo tra l'UE e gli Stati Uniti («USA»).

Secondo la Corte, i requisiti della normativa interna degli Stati Uniti, e in particolare taluni programmi che consentono l'accesso da parte delle autorità pubbliche statunitensi, per finalità di sicurezza nazionale, ai dati personali trasferiti dall'Unione europea verso gli Stati Uniti, comportano limitazioni della protezione dei dati personali che non sono configurate in modo da soddisfare requisiti sostanzialmente equivalenti a quelli richiesti nel diritto dell'Unione (1); inoltre,

tale normativa non conferisce agli interessati diritti azionabili in sede giudiziaria nei confronti delle autorità statunitensi.

Alla luce di tale grado di ingerenza nei diritti fondamentali delle persone i cui dati sono trasferiti verso tale paese terzo, la Corte ha dichiarato invalida la decisione sull'adeguatezza dello scudo per la privacy.

2. La sentenza della Corte ha implicazioni su strumenti di trasferimento diversi dallo scudo per la privacy?

In generale, per i paesi terzi, la soglia fissata dalla Corte si applica anche a tutte le garanzie adeguate di cui all'articolo 46 del RGPD, utilizzate per il trasferimento dei dati dal SEE a qualsiasi paese terzo. La normativa statunitense richiamata dalla Corte [l'articolo 702 del Foreign Intelligence Surveillance Act (FISA) e l'Executive Order (EO) 12333] si applica a qualsiasi trasferimento verso gli Stati Uniti eseguito con mezzi elettronici che rientri nell'ambito di applicazione della suddetta normativa, a prescindere dallo strumento utilizzato per il trasferimento (²).

3. È previsto un periodo di tolleranza durante il quale si può continuare a trasferire i dati verso gli Stati Uniti senza valutare la base giuridica per il trasferimento?

No, la Corte ha invalidato la decisione sullo scudo per la privacy senza preservarne gli effetti, poiché la normativa statunitense oggetto della valutazione della Corte non fornisce un livello di protezione sostanzialmente equivalente a quello dell'Unione. Di questa valutazione si deve tenere conto con riguardo a qualsiasi trasferimento verso gli Stati Uniti.

4. Trasferivo i dati a un importatore di dati statunitense aderente allo scudo per la privacy, che cosa devo fare ora?

I trasferimenti sulla base di questo quadro giuridico sono illegali. Qualora si desideri continuare a trasferire i dati verso gli Stati Uniti, è necessario verificare se ciò sia possibile alle condizioni stabilite in appresso.

5. Sto utilizzando clausole contrattuali tipo con un importatore di dati negli Stati Uniti, che cosa devo fare?

La Corte ha rilevato che la legislazione statunitense (ossia l'articolo 702 del FISA e l'EO 12333) non garantisce un livello di protezione sostanzialmente equivalente.

La possibilità di trasferire dati personali sulla base delle clausole contrattuali tipo dipenderà dall'esito della valutazione condotta, tenendo conto delle circostanze dei trasferimenti e delle misure supplementari eventualmente attuabili. Le misure supplementari unitamente alle clausole contrattuali tipo, previa analisi caso per caso delle circostanze del trasferimento, dovrebbero assicurare che la normativa statunitense non interferisca con il livello di protezione adeguato dalle stesse garantito.

Qualora si giunga alla conclusione che, tenuto conto delle circostanze del trasferimento e delle possibili misure supplementari, non sarebbero assicurate garanzie adeguate, vi è l'obbligo di sospendere o cessare il trasferimento dei dati personali. Se si intende tuttavia proseguire col trasferimento dei dati malgrado la suddetta conclusione, è obbligatorio informarne l'autorità di controllo competente ([3]).

6. Sto utilizzando norme d'impresa vincolanti (BCR) con un soggetto stabilito negli Stati Uniti, che cosa devo fare?

In considerazione della sentenza della Corte, che ha invalidato lo scudo per la privacy a causa del grado di ingerenza creato dalla normativa statunitense nei diritti fondamentali delle persone i cui dati sono trasferiti verso tale paese terzo, e alla luce della circostanza per cui lo scudo per la privacy è stato concepito anche per fornire garanzie ai dati trasferiti con altri strumenti, quali le norme vincolanti d'impresa, la valutazione della Corte si applica anche nel contesto delle norme vincolanti d'impresa, poiché la normativa statunitense prevarrà anche su quest'ultimo strumento.

La possibilità di trasferire i dati personali sulla base delle norme vincolanti d'impresa dipenderà dal risultato della valutazione effettuata, tenendo conto delle circostanze dei trasferimenti e delle misure supplementari eventualmente attuabili. Tali misure supplementari unitamente alle norme vincolanti d'impresa, previa analisi caso per caso delle circostanze del trasferimento, dovrebbero assicurare che la normativa statunitense non interferisca con il livello di protezione adeguato dalle stesse garantito.

Qualora si giunga alla conclusione che, tenuto conto delle circostanze del trasferimento e delle possibili misure supplementari, non sarebbero assicurate garanzie adeguate, vi è l'obbligo di sospendere o cessare il trasferimento dei dati personali. Se si intende ciononostante proseguire col trasferimento dei dati, è obbligatorio informare l'autorità di controllo competente ([4]).

7. Che cosa è previsto per gli altri strumenti di trasferimento ai sensi dell'articolo 46 del RGPD?

L'EDPB valuterà le conseguenze della sentenza sugli strumenti di trasferimento diversi dalle clausole contrattuali tipo e dalle norme vincolanti d'impresa. La sentenza chiarisce che lo standard per l'adeguatezza delle garanzie ai sensi dell'articolo 46 del RGPD è costituito dalla «equivalenza sostanziale».

Come evidenziato dalla Corte, l'articolo 46 figura nel capo V del RGPD e, di conseguenza, deve essere letto alla luce dell'articolo 44 del regolamento stesso, in base al quale «*tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato*».

8. Posso utilizzare le deroghe previste dall'articolo 49 del RGPD per il trasferimento di dati verso gli Stati Uniti?

Il trasferimento dei dati dal SEE agli Stati Uniti sulla base delle deroghe previste dall'articolo 49 del RGPD è ancora possibile, purché siano soddisfattele condizioni stabilite in tale articolo. L'EDPB rimanda alle proprie linee guida sul punto ([5]).

Va ricordato, in particolare, che quando i trasferimenti si basano sul consenso dell'interessato, tale consenso deve essere:

- esplicito,
- specifico con riguardo al trasferimento o al complesso di trasferimenti di dati in questione (ciò significa che l'esportatore deve assicurarsi di ricevere un consenso specifico prima di mettere in atto il trasferimento, anche se ciò avviene dopo la raccolta dei dati) e
- informato, soprattutto rispetto ai possibili rischi del trasferimento (ciò significa che l'interessato deve essere informato anche dei rischi specifici derivanti dal trasferimento verso un paese terzo che non offre una protezione adeguata, e dell'assenza di adeguate garanzie per la protezione dei dati).

Per quanto concerne i trasferimenti necessari all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento, va ricordato che i dati personali possono essere trasferiti soltanto su base occasionale. Il carattere «occasionale» o «non occasionale» dei trasferimenti deve essere stabilito caso per caso. Questa deroga può comunque essere applicata soltanto se il trasferimento è oggettivamente necessario per l'esecuzione del contratto.

In relazione ai trasferimenti necessari per importanti motivi di interesse pubblico [che devono essere riconosciuti dal diritto dell'Unione o dal diritto degli Stati membri ([6])], l'EDPB ricorda che il requisito essenziale per l'applicabilità di questa deroga risiede nella constatazione della sussistenza di un motivo di interesse pubblico rilevante e non nella natura del soggetto coinvolto nel trasferimento, e che, sebbene la deroga non si limiti ai trasferimenti di dati «occasionali», ciò non significa che, in base alla deroga per importanti motivi di interesse pubblico, possano avere luogo trasferimenti di dati sistematici e su larga scala. Occorre semmai rispettare il principio generale secondo cui le deroghe stabilite nell'articolo 49 del RGPD non dovrebbero trasformarsi di fatto in una regola, essendo necessario limitarne l'applicazione a situazioni specifiche e purché ogni esportatore di dati garantisca che il trasferimento soddisfa un rigoroso test di necessità.

9. Posso continuare a utilizzare le clausole contrattuali tipo o le norme vincolanti d'impresa per il trasferimento dei dati verso un paese terzo diverso dagli Stati Uniti?

La Corte ha indicato che, di norma, le clausole contrattuali tipo possono ancora essere utilizzate per il trasferimento di dati verso un paese terzo; tuttavia, la soglia fissata dalla Corte per i trasferimenti verso gli Stati Uniti si applica a qualsiasi paese terzo. Lo stesso vale per le norme vincolanti d'impresa.

La Corte ha sottolineato che spetta all'esportatore e all'importatore dei dati verificare il rispetto, nel paese terzo, del livello di protezione richiesto dal diritto dell'Unione, al fine di determinare se le garanzie previste dalle clausole contrattuali tipo o dalle norme vincolanti d'impresa possano essere rispettate nella pratica. In caso contrario, occorre accertare se sia possibile prevedere misure supplementari atte a garantire un livello di protezione sostanzialmente equivalente a quello vigente nel SEE, e se il diritto del paese terzo non consenta ingerenze nei riguardi delle suddette misure supplementari tali da comprometterne di fatto l'efficacia.

È possibile contattare l'importatore dei dati per verificare la legislazione del rispettivo paese e collaborare alla necessaria valutazione. Qualora si stabilisca, da parte dell'esportatore o dell'importatore nel paese terzo, che il livello di protezione previsto per i dati trasferiti ai sensi delle clausole contrattuali tipo o delle norme vincolanti d'impresa non è sostanzialmente equivalente a quello garantito all'interno del SEE, i trasferimenti devono essere immediatamente sospesi. In caso contrario, occorre informarne l'autorità di controllo competente (7).

Sebbene, come sottolineato dalla Corte, sia responsabilità primaria degli esportatori e degli importatori accertarsi che la legislazione del paese terzo di destinazione consenta all'importatore di rispettare le clausole tipo di protezione dei dati o le norme vincolanti d'impresa, prima di procedere al trasferimento dei dati personali verso tale paese terzo, anche le autorità di controllo avranno da svolgere un ruolo fondamentale nell'attuazione del RGPD e nell'adozione di ulteriori decisioni in merito ai trasferimenti verso paesi terzi.

Come sollecitato dalla Corte, al fine di evitare decisioni divergenti, le autorità di controllo sono chiamate a proseguire la collaborazione in seno all'EDPB per garantire approcci coerenti, in particolare qualora debbano essere vietati determinati trasferimenti verso paesi terzi.

10. Quali misure supplementari posso introdurre se utilizzo clausole contrattuali tipo o norme vincolanti d'impresa per il trasferimento di dati verso paesi terzi?

Le misure supplementari eventualmente da introdurre, ove necessario, dovrebbero essere stabilite caso per caso, tenendo conto di tutte le circostanze del trasferimento e previa valutazione della legislazione del paese terzo, al fine di verificare se essa assicuri un livello di protezione adeguato.

La Corte ha sottolineato che è responsabilità primaria dell'esportatore e dell'importatore effettuare tale valutazione e fornire le misure supplementari necessarie.

L'EDPB sta analizzando la sentenza della Corte per stabilire quali misure supplementari, di natura giuridica, tecnica o organizzativa, potrebbero essere previste in aggiunta alle clausole contrattuali tipo o alle norme vincolanti d'impresa per il trasferimento dei dati verso paesi terzi in cui dette clausole o norme non offrono isolatamente un livello sufficiente di garanzie.

L'EDPB intende approfondire l'analisi relativa alla tipologia delle misure supplementari e fornirà ulteriori indicazioni in merito.

11. Mi avvalgo di un responsabile del trattamento per dati di cui io sono il titolare, come posso sapere se tale responsabile trasferisce i dati verso gli Stati Uniti o un altro paese terzo?

Il contratto concluso con un responsabile del trattamento a norma dell'articolo 28, paragrafo 3, del RGPD, deve stabilire se i trasferimenti siano autorizzati o meno (si tenga presente che anche fornire accesso ai dati da un paese terzo, ad esempio per finalità amministrative, costituisce un trasferimento).

Occorre un'autorizzazione anche per consentire a responsabili del trattamento di affidare a sub-responsabili il trasferimento dei dati verso paesi terzi. È necessario prestare attenzione e usare cautela poiché numerose soluzioni informatiche possono comportare il trasferimento di dati personali verso un paese terzo (ad esempio, per scopi di conservazione o manutenzione).

12. Cosa posso fare per continuare ad avvalermi dei servizi del responsabile del trattamento se il contratto firmato in conformità dell'articolo 28.3 del RGPD indica la possibilità di trasferire i dati verso gli Stati Uniti o un altro paese terzo?

Qualora sia previsto che i dati siano trasferiti verso gli Stati Uniti e non siano ipotizzabili misure supplementari atte a garantire che la normativa statunitense non incida sul livello di protezione sostanzialmente equivalente a quello garantito nel SEE assicurato dagli strumenti di trasferimento, né si applichino le deroghe di cui all'articolo 49 del RGPD, l'unica soluzione è negoziare un emendamento o una clausola supplementare al contratto al fine di vietare i trasferimenti verso gli Stati Uniti. Non solo la conservazione, ma anche la gestione dei dati dovrebbero quindi avvenire in un luogo diverso dagli Stati Uniti.

Nel caso in cui i dati possano essere trasferiti verso un altro paese terzo, è necessario verificare anche la legislazione di tale paese terzo per accertarne la conformità ai requisiti della Corte e al livello di protezione dei dati personali atteso. Qualora sia impossibile individuare un'idonea base giuridica per il trasferimento verso un paese terzo, non si dovrebbe procedere ad alcun trasferimento di dati personali al di fuori del territorio del SEE e tutte le attività di trattamento dovrebbero avere luogo all'interno del SEE.

Per il comitato europeo per la protezione dei dati
La presidente

Andrea Jelinek

NOTE

[1] La Corte rileva che taluni programmi di sorveglianza che consentono l'accesso da parte delle autorità pubbliche statunitensi, per finalità di sicurezza nazionale, ai dati personali trasferiti dall'Unione europea verso gli Stati Uniti non prevedono limitazioni al potere conferito alle autorità statunitensi, e neppure garanzie per gli stranieri potenzialmente oggetto di tale sorveglianza.

[2] L'articolo 702 del FISA si applica a tutti i «fornitori di servizi di comunicazione elettronica» [si veda la definizione al 50 USC § 1881(b)(4)], mentre l'EO 12 333 disciplina la sorveglianza elettronica, definita come «l'acquisizione di una comunicazione non pubblica con mezzi elettronici senza il consenso di una persona che è parte di una comunicazione elettronica o, in caso di comunicazione non elettronica, senza il consenso di una persona visibilmente presente nel luogo della comunicazione, ad esclusione dell'uso di apparecchiature radiogoniometriche al solo scopo di determinare la posizione di un trasmettitore» [3.4; b)].

[3] Si vedano in particolare il considerando 145 della sentenza della Corte e la clausola 4, lettera g), della decisione della Commissione 2010/87/UE, nonché la clausola 5, lettera a) della decisione della Commissione 2001/497/CE e l'insieme II, lettera c), dell'allegato della decisione della Commissione 2004/915/CE.

[4] Si vedano in particolare il considerando 145 della sentenza della Corte e la clausola 4, lettera g), della decisione della Commissione 2010/87/UE. Si vedano anche la sezione 6.3, WP256 rev.01 (Gruppo di lavoro «articolo 29», documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa, adottato dall'EDPB, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109) e la sezione 6.3, WP257 rev.01 (Gruppo di lavoro «articolo 29», documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa per i responsabili del trattamento, adottato dall'EDPB, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110).

[5] Si vedano le Linee guida 2/2018 del comitato europeo per la protezione dei dati sulle deroghe di cui all'articolo 49 del regolamento 2016/679, adottate il 25 maggio 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_it.pdf, pag. 3.

[6] Con il termine «Stati membri» si intendono gli «Stati membri del SEE».

[7] Si veda in particolare il punto 145 della sentenza della Corte. In relazione alle clausole contrattuali tipo, si vedano la clausola 4, lettera g), della decisione della Commissione 2010/87/UE, nonché la clausola 5, lettera a) della decisione della Commissione 2001/497/CE e l'allegato II, lettera c), della decisione della Commissione 2004/915/CE. In relazione alle norme vincolanti d'impresa, si vedano la sezione 6.3 WP256 rev.01 (approvato dall'EDPB) e la sezione 6.3 WP257 rev.01 (approvato dall'EDPB).

DECISIONE DI ESECUZIONE (UE) 2021/914 DELLA COMMISSIONE

del 4 giugno 2021

relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) ([1]), in particolare l'articolo 28, paragrafo 7, e l'articolo 46, paragrafo 2, lettera c),

considerando quanto segue:

(1) Gli sviluppi tecnologici facilitano i flussi transfrontalieri di dati necessari per l'espansione della cooperazione internazionale e del commercio internazionale. Nel contempo occorre assicurare che il livello di protezione delle persone fisiche garantito dal regolamento (UE) 2016/679 non sia pregiudicato qualora i dati personali siano trasferiti verso paesi terzi, anche in caso di trasferimenti successivi ([2]). Le disposizioni sui trasferimenti di dati di cui al capo V del regolamento (UE) 2016/679 sono intese a garantire la continuità di tale livello elevato di protezione quando i dati personali sono trasferiti verso un paese terzo ([3]).

(2) In conformità dell'articolo 46, paragrafo 1, del regolamento (UE) 2016/679, in mancanza di una decisione di adeguatezza della Commissione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Possono costituire siffatte garanzie le clausole tipo di protezione dei dati adottate dalla Commissione a norma dell'articolo 46, paragrafo 2, lettera c).

(3) Il ruolo delle clausole contrattuali tipo è limitato ad assicurare garanzie adeguate in materia di protezione dei dati per i trasferimenti internazionali di dati. Pertanto, il titolare del trattamento o il responsabile del trattamento che trasferisce i dati personali verso un paese terzo («esportatore») e il titolare del trattamento o il responsabile del trattamento che riceve i dati personali («importatore») sono liberi di includere tali clausole contrattuali tipo in un contratto più ampio e di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo o pregiudichino i diritti o le libertà fondamentali degli interessati. I titolari del trattamento e i responsabili del trattamento sono incoraggiati a fornire garanzie supplementari attraverso impegni contrattuali che integrino le clausole contrattuali tipo ([4]). L'utilizzo delle clausole contrattuali tipo lascia impregiudicato qualunque obbligo contrattuale dell'esportatore e/o dell'importatore di garantire il rispetto dei privilegi e delle immunità applicabili.

(4) Oltre ad utilizzare clausole contrattuali tipo per fornire garanzie adeguate per i trasferimenti in conformità dell'articolo 46, paragrafo 1, del regolamento (UE) 2016/679, l'esportatore deve adempiere alle responsabilità generali che gli incombono in quanto titolare del trattamento o responsabile del trattamento a norma del regolamento (UE) 2016/679. Tali responsabilità comprendono l'obbligo del titolare del trattamento di fornire agli interessati informazioni in merito alla sua intenzione di trasferire i dati personali verso un paese terzo in conformità dell'articolo 13, paragrafo 1, lettera f), e dell'articolo 14, paragrafo 1, lettera f), del regolamento (UE) 2016/679. Nel caso di trasferimenti in conformità dell'articolo 46 del regolamento (UE) 2016/679, tali informazioni devono includere un riferimento alle garanzie adeguate e ai mezzi per ottenere una copia di tali dati o informazioni sul luogo dove sono stati resi disponibili.

([1]) GU L 119 del 4.5.2016, pag. 1.
([2]) Articolo 44 del regolamento (UE) 2016/679.
([3]) Cfr. anche la sentenza della Corte di giustizia del 16 luglio 2020 nella causa C-311/18, *Data Protection Commissioner* contro *Facebook Ireland Ltd e Maximillian Schrems ("Schrems II")*, ECLI:EU:C:2020:559, punto 93.
([4]) Considerando 109 del regolamento (UE) 2016/679.

(5) La decisione 2001/497/CE della Commissione ([5]) e la decisione 2010/87/UE della Commissione ([6]) contengono clausole contrattuali tipo per facilitare il trasferimento di dati personali da un titolare del trattamento stabilito nell'Unione a un titolare del trattamento o un responsabile del trattamento stabilito in un paese terzo che non offre un livello di protezione adeguato. Tali decisioni si basavano sulla direttiva 95/46/CE del Parlamento europeo e del Consiglio ([7]).

(6) In conformità dell'articolo 46, paragrafo 5, del regolamento (UE) 2016/679, la decisione 2001/497/CE e la decisione 2010/87/UE restano in vigore fino a quando non vengono modificate, sostituite o abrogate, se necessario, da una decisione della Commissione adottata a norma dell'articolo 46, paragrafo 2, del medesimo regolamento. Le clausole contrattuali tipo contenute nelle decisioni hanno reso necessario un aggiornamento alla luce dei nuovi requisiti di cui al regolamento (UE) 2016/679. Inoltre, dall'adozione di tali decisioni si sono verificati importanti sviluppi nell'economia digitale, con l'uso diffuso di nuovi e più complessi trattamenti che coinvolgono spesso numerosi importatori ed esportatori, lunghe e complesse catene di trattamento e relazioni commerciali in evoluzione. Ciò richiede una modernizzazione delle clausole contrattuali tipo per rispecchiare meglio tali realtà, contemplando ulteriori situazioni di trattamento e trasferimento, e consentire un approccio più flessibile, ad esempio per quanto riguarda il numero di parti che possono aderire al contratto.

(7) Il titolare del trattamento o il responsabile del trattamento può utilizzare le clausole contrattuali tipo figuranti nell'allegato della presente decisione per fornire garanzie adeguate ai sensi dell'articolo 46, paragrafo 1, del regolamento (UE) 2016/679 ai fini del trasferimento di dati personali a un responsabile del trattamento o a un titolare del trattamento stabilito in un paese terzo, fatta salva l'interpretazione della nozione di trasferimento internazionale ai sensi del regolamento (UE) 2016/679. Le clausole contrattuali tipo possono essere utilizzate per tali trasferimenti soltanto nella misura in cui il trattamento da parte dell'importatore non rientri nell'ambito di applicazione del regolamento (UE) 2016/679. Ciò comprende anche il trasferimento di dati personali ad opera di un titolare del trattamento o un responsabile del trattamento che non è stabilito nell'Unione, nella misura in cui il trattamento sia soggetto al regolamento (UE) 2016/679 (in conformità dell'articolo 3, paragrafo 2, del medesimo), in quanto si riferisce all'offerta di beni o servizi ad interessati nell'Unione o al monitoraggio del loro comportamento nella misura in cui questo abbia luogo all'interno dell'Unione.

(8) Dato l'allineamento generale del regolamento (UE) 2016/679 e del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([8]), dovrebbe essere possibile utilizzare le clausole contrattuali tipo anche nel contesto di un contratto di cui all'articolo 29, paragrafo 4, del regolamento (UE) 2018/1725 per il trasferimento di dati personali a un sub-responsabile del trattamento in un paese terzo ad opera di un responsabile del trattamento che non sia un'istituzione o un organo dell'Unione ma che sia soggetto al regolamento (UE) 2016/679 e che tratti dati personali per conto di un'istituzione o di un organo dell'Unione conformemente all'articolo 29 del regolamento (UE) 2018/1725. A condizione che il contratto rifletta gli stessi obblighi in materia di protezione dei dati stabiliti nel contratto o altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento in conformità dell'articolo 29, paragrafo 3, del regolamento (UE) 2018/1725, in particolare fornendo garanzie sufficienti per le misure tecniche e organizzative volte ad assicurare che il trattamento soddisfi i requisiti di tale regolamento, ciò garantirà il rispetto dell'articolo 29, paragrafo 4, del regolamento (UE) 2018/1725. Si tratta, segnatamente, del caso in cui il titolare del trattamento e il responsabile del trattamento utilizzano le clausole contrattuali tipo stabilite nella decisione di esecuzione della Commissione relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([9]).

(9) Qualora il trattamento comporti trasferimenti di dati da titolari del trattamento soggetti al regolamento (UE) 2016/679 a responsabili del trattamento che non rientrano nell'ambito di applicazione territoriale di tale regolamento, o da responsabili del trattamento soggetti al regolamento (UE) 2016/679 a sub-responsabili del trattamento che non rientrano nell'ambito di applicazione territoriale di tale regolamento, le clausole contrattuali tipo figuranti nell'allegato della presente decisione dovrebbero consentire di soddisfare anche i requisiti di cui all'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679.

(10) Le clausole contrattuali tipo figuranti nell'allegato della presente decisione combinano clausole generali con un approccio modulare per rispondere ai diversi scenari di trasferimento e alla complessità delle moderne catene di trattamento. Oltre alle clausole generali, i titolari del trattamento e i responsabili del trattamento dovrebbero scegliere il modulo applicabile alla loro situazione, in modo da adattare gli obblighi derivanti dalle clausole

([5]) Decisione 2001/497/CE della Commissione, del 15 giugno 2001, relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE (GU L 181 del 4.7.2001, pag. 19).

([6]) Decisione 2010/87/UE della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio (GU L 39 del 12.2.2010, pag. 5).

([7]) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

([8]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39); cfr. il considerando 5.

([9]) C(2021) 3701 final.

contrattuali tipo al loro ruolo e alle loro responsabilità in relazione al trattamento di dati in questione. Alle clausole contrattuali tipo dovrebbero poter aderire più di due parti. Inoltre, dovrebbe essere consentito a ulteriori titolari del trattamento e responsabili del trattamento di aderire alle clausole contrattuali tipo in qualità di esportatori o importatori durante l'intero ciclo di vita del contratto di cui tali clausole fanno parte.

(11) Al fine di offrire garanzie adeguate, le clausole contrattuali tipo dovrebbero assicurare che ai dati personali trasferiti sulla loro base sia assicurato un livello di protezione sostanzialmente equivalente a quello assicurato all'interno dell'Unione ([10]). Per garantire la trasparenza del trattamento, gli interessati dovrebbero ricevere una copia delle clausole contrattuali tipo ed essere informati, in particolare, delle categorie di dati personali trattati, del diritto di ottenere una copia delle clausole contrattuali tipo e di eventuali trasferimenti successivi. I trasferimenti successivi dall'importatore a un terzo in un altro paese terzo dovrebbero essere consentiti solo se il terzo aderisce alle clausole contrattuali tipo, se la continuità della protezione è garantita in altro modo, o in situazioni specifiche, ad esempio sulla base del consenso esplicito e informato dell'interessato.

(12) Con alcune eccezioni, in particolare per quanto concerne determinati obblighi che riguardano esclusivamente il rapporto tra l'esportatore e l'importatore, gli interessati dovrebbero poter invocare e, se necessario far valere, le clausole contrattuali tipo in qualità di terzi beneficiari. Pertanto, anche se le parti devono poter scegliere la legge di uno degli Stati membri quale legge applicabile alle clausole contrattuali tipo, tale legge deve prevedere i diritti del terzo beneficiario. Al fine di facilitare il ricorso individuale, le clausole contrattuali tipo dovrebbero imporre all'importatore di informare gli interessati circa un punto di contatto e di trattare prontamente eventuali reclami o richieste. In caso di controversia tra l'importatore e un interessato che invochi i propri diritti in qualità di terzo beneficiario, l'interessato dovrebbe poter proporre reclamo all'autorità di controllo competente o deferire la controversia agli organi giurisdizionali competenti dell'UE.

(13) Al fine di garantire un'applicazione efficace, l'importatore dovrebbe essere tenuto a sottoporsi alla giurisdizione di tali autorità e organi giurisdizionali e a impegnarsi ad attenersi a qualunque decisione vincolante a norma della legislazione applicabile dello Stato membro. In particolare, l'importatore dovrebbe accettare di rispondere alle richieste di informazioni, sottoporsi ad attività di revisione e rispettare le misure adottate dall'autorità di controllo, comprese le misure di riparazione e risarcimento. Inoltre, l'importatore dovrebbe avere l'opzione di offrire agli interessati la possibilità di rivolgersi gratuitamente a un organismo indipendente di risoluzione delle controversie. In linea con l'articolo 80, paragrafo 1, del regolamento (UE) 2016/679, gli interessati dovrebbero essere autorizzati a farsi rappresentare, se lo desiderano, da associazioni o altri organismi nelle controversie contro l'importatore.

(14) Le clausole contrattuali tipo dovrebbero prevedere norme sulla responsabilità tra le parti e nei confronti degli interessati, e norme sull'indennizzo tra le parti. Qualora subisca un danno materiale o immateriale causato da una violazione dei diritti del terzo beneficiario derivanti dalle clausole contrattuali tipo, l'interessato dovrebbe avere diritto al risarcimento. Ciò dovrebbe lasciare impregiudicata qualunque responsabilità ai sensi del regolamento (UE) 2016/679.

(15) In caso di trasferimento a un importatore che agisce in qualità di responsabile del trattamento o sub-responsabile del trattamento, dovrebbero applicarsi requisiti specifici conformemente all'articolo 28, paragrafo 3, del regolamento (UE) 2016/679. Le clausole contrattuali tipo dovrebbero imporre all'importatore di mettere a disposizione tutte le informazioni necessarie per dimostrare il rispetto degli obblighi stabiliti dalle clausole e di consentire e contribuire alle attività di revisione delle sue attività di trattamento da parte dell'esportatore. Per quanto riguarda il ricorso dell'importatore a un sub-responsabile del trattamento, conformemente all'articolo 28, paragrafi 2 e 4, del regolamento (UE) 2016/679, le clausole contrattuali tipo dovrebbero stabilire in particolare la procedura per l'autorizzazione generale o specifica da parte dell'esportatore e il requisito di un contratto scritto con il sub-responsabile del trattamento che garantisca lo stesso livello di protezione previsto dalle clausole.

(16) È opportuno prevedere nelle clausole contrattuali tipo garanzie diverse che coprano la situazione specifica di un trasferimento di dati personali da un responsabile del trattamento nell'Unione al suo titolare del trattamento in un paese terzo, e che rispecchino i limitati obblighi autonomi per i responsabili del trattamento a norma del regolamento (UE) 2016/679. In particolare, le clausole contrattuali tipo dovrebbero fare obbligo al responsabile del trattamento di informare il titolare del trattamento qualora non sia in grado di seguire le sue istruzioni, compreso se tali istruzioni violano la legislazione dell'Unione in materia di protezione dei dati, e al titolare del trattamento di astenersi da qualunque azione che impedisca al responsabile del trattamento di adempiere ai propri obblighi a norma del regolamento (UE) 2016/679. Dovrebbero inoltre imporre alle parti di prestarsi reciproca assistenza nel rispondere alle richieste di informazioni e alle richieste presentate dagli interessati a norma della legislazione locale applicabile all'importatore o, per il trattamento dei dati nell'Unione, a norma del regolamento (UE) 2016/679. Qualora il responsabile del trattamento dell'Unione combini i dati personali ricevuti dal titolare del trattamento del

([10]) *Schrems II*, punti 96 e 103. Cfr. anche il regolamento (UE) 2016/679, considerando 108 e 114.

paese terzo con dati personali che ha raccolto nell'Unione, si dovrebbero applicare ulteriori requisiti per far fronte a eventuali effetti della legislazione del paese terzo di destinazione sul rispetto delle clausole da parte del titolare del trattamento, in particolare per quanto riguarda il modo in cui trattare le richieste vincolanti di autorità pubbliche del paese terzo di comunicare i dati personali trasferiti. Per contro, tali requisiti non sono giustificati quando l'esternalizzazione comporta unicamente il trattamento e il ritrasferimento di dati personali che sono stati ricevuti dal titolare del trattamento e che, in ogni caso, sono stati e rimarranno soggetti alla giurisdizione del paese terzo in questione.

(17) Le parti dovrebbero essere in grado di dimostrare il rispetto delle clausole contrattuali tipo. In particolare, l'importatore dovrebbe essere tenuto a conservare documentazione adeguata delle attività di trattamento sotto la sua responsabilità e a informare prontamente l'esportatore qualora, per qualunque motivo, non sia in grado di rispettare le clausole. A sua volta, l'esportatore dovrebbe sospendere il trasferimento e, nei casi particolarmente gravi, avere il diritto di risolvere il contratto, per quanto riguarda il trattamento di dati personali nell'ambito delle clausole contrattuali tipo, qualora l'importatore violi le clausole o non sia in grado di rispettarle. Si dovrebbero applicare norme specifiche qualora la legislazione locale incida sul rispetto delle clausole. I dati personali che sono stati trasferiti prima della risoluzione del contratto e le loro eventuali copie dovrebbero, a scelta dell'esportatore, essere restituiti all'esportatore o distrutti integralmente.

(18) Le clausole contrattuali tipo dovrebbero prevedere garanzie specifiche, in particolare alla luce della giurisprudenza della Corte di giustizia ([11]), per far fronte a eventuali effetti della legislazione del paese terzo di destinazione sul rispetto delle clausole da parte dell'importatore, in particolare per quanto riguarda il modo in cui trattare le richieste vincolanti di autorità pubbliche del paese terzo di comunicare i dati personali trasferiti.

(19) Il trasferimento e il trattamento dei dati personali nell'ambito delle clausole contrattuali tipo non dovrebbero aver luogo se la legislazione e le prassi del paese terzo di destinazione impediscono all'importatore di rispettare le clausole. In tale contesto, la legislazione e le prassi che rispettano l'essenza dei diritti e delle libertà fondamentali e non vanno oltre quanto necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi di cui all'articolo 23, paragrafo 1, del regolamento (UE) 2016/679 non dovrebbero ritenersi in conflitto con le clausole contrattuali tipo. Le parti dovrebbero garantire che, al momento dell'accettazione delle clausole contrattuali tipo, non hanno motivo di ritenere che la legislazione e le prassi applicabili all'importatore non sono in linea con tali requisiti.

(20) Le parti dovrebbero tenere conto in particolare delle circostanze specifiche del trasferimento (quali il contenuto e la durata del contratto, la natura dei dati da trasferire, il tipo di destinatario, la finalità del trattamento), della legislazione e delle prassi del paese terzo di destinazione pertinenti alla luce delle circostanze del trasferimento, e delle eventuali garanzie messe in atto per integrare le garanzie previste dalle clausole contrattuali tipo (comprese le pertinenti misure contrattuali, tecniche e organizzative che si applicano alla trasmissione e al trattamento dei dati personali nel paese di destinazione). Per quanto riguarda l'impatto della legislazione e delle prassi sul rispetto delle clausole contrattuali tipo, possono essere presi in considerazione diversi elementi nell'ambito di una valutazione globale, tra cui informazioni affidabili sull'applicazione pratica della legislazione (come la giurisprudenza e le relazioni di organismi di vigilanza indipendenti), l'esistenza o l'assenza di richieste nello stesso settore e, in condizioni rigorose, l'esperienza pratica documentata dell'esportatore e/o dell'importatore.

(21) L'importatore dovrebbe informare l'esportatore se, dopo aver accettato le clausole contrattuali tipo, ha motivo di ritenere di non essere in grado di rispettarle. Se riceve tale notifica o viene altrimenti a conoscenza del fatto che l'importatore non è più in grado di rispettare le clausole contrattuali tipo, l'esportatore dovrebbe individuare le misure appropriate per far fronte alla situazione, se necessario in consultazione con l'autorità di controllo competente. Tali misure possono comprendere l'adozione di misure supplementari ad opera dall'esportatore e/o dell'importatore, quali misure tecniche o organizzative per garantire la sicurezza e la riservatezza. L'esportatore dovrebbe essere tenuto a sospendere il trasferimento se ritiene che non possano essere assicurate garanzie adeguate o su istruzione dell'autorità di controllo competente.

([11]) *Schrems II*.

(22) Se riceve una richiesta giuridicamente vincolante di un'autorità pubblica (anche giudiziaria), a norma della legislazione del paese di destinazione, di comunicare dati personali trasferiti in conformità delle clausole contrattuali tipo, l'importatore dovrebbe informarne l'esportatore e l'interessato, ove possibile. Analogamente, dovrebbe informarli se viene a conoscenza di un accesso diretto a tali dati personali da parte di autorità pubbliche, conformemente alla legislazione del paese terzo di destinazione. Se, pur avendo fatto tutto il possibile, non è in grado di informare l'esportatore e/o l'interessato di specifiche richieste di comunicazione, l'importatore dovrebbe fornire all'esportatore quante più informazioni pertinenti possibili sulle richieste. Inoltre dovrebbe fornire periodicamente all'esportatore informazioni aggregate. L'importatore dovrebbe altresì essere tenuto a documentare tutte le richieste di comunicazione ricevute e le risposte fornite e a mettere tali informazioni a disposizione dell'esportatore o dell'autorità di controllo competente, o di entrambi, su richiesta. Se, a seguito di un riesame della legittimità di una siffatta richiesta a norma della legislazione del paese di destinazione, conclude che sussistono fondati motivi per ritenere che essa sia illegittima a norma della legislazione del paese terzo di destinazione, l'importatore dovrebbe contestarla, se del caso anche esaurendo le possibilità di ricorso disponibili. In ogni caso, se non è più in grado di rispettare le clausole contrattuali tipo, l'importatore dovrebbe informarne l'esportatore, anche qualora tale incapacità sia la conseguenza di una richiesta di comunicazione.

(23) Poiché le esigenze dei portatori di interessi, la tecnologia e i trattamenti possono cambiare, la Commissione dovrebbe valutare il funzionamento delle clausole contrattuali tipo alla luce dell'esperienza, nell'ambito della valutazione periodica del regolamento (UE) 2016/679 prevista all'articolo 97 di tale regolamento.

(24) La decisione 2001/497/CE e la decisione 2010/87/UE dovrebbero essere abrogate tre mesi dopo l'entrata in vigore della presente decisione. Durante tale periodo gli esportatori e gli importatori dovrebbero, ai fini dell'articolo 46, paragrafo 1, del regolamento (UE) 2016/679, poter continuare a utilizzare le clausole contrattuali tipo di cui alle decisioni 2001/497/CE e 2010/87/UE. Per un ulteriore periodo di 15 mesi, gli esportatori e gli importatori dovrebbero, ai fini dell'articolo 46, paragrafo 1, del regolamento (UE) 2016/679, poter continuare a basarsi sulle clausole contrattuali tipo di cui alle decisioni 2001/497/CE e 2010/87/UE per l'esecuzione di contratti conclusi tra loro prima della data di abrogazione di tali decisioni, purché i trattamenti oggetto dei contratti rimangano invariati e il ricorso alle clausole garantisca che il trasferimento di dati personali sia soggetto a garanzie adeguate ai sensi dell'articolo 46, paragrafo 1, del regolamento (UE) 2016/679. In caso di modifiche rilevanti del contratto, l'esportatore dovrebbe essere tenuto a basarsi su un nuovo fondamento per i trasferimenti di dati in virtù del contratto, in particolare sostituendo le clausole contrattuali tipo esistenti con le clausole contrattuali tipo figuranti nell'allegato della presente decisione. Lo stesso dovrebbe valere per qualunque subcontratto che affidi i trattamenti oggetto del contratto a un (sub-)responsabile del trattamento.

(25) Il garante europeo della protezione dei dati e il comitato europeo per la protezione dei dati sono stati consultati a norma dell'articolo 42, paragrafi 1 e 2, del regolamento (UE) 2018/1725 e hanno espresso un parere congiunto il 14 gennaio 2021 ([12]), di cui si è tenuto conto nella preparazione della presente decisione.

(26) Le misure di cui alla presente decisione sono conformi al parere del comitato istituito a norma dell'articolo 93 del regolamento (UE) 2016/679,]

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

1. Le clausole contrattuali tipo figuranti in allegato sono ritenute fornire garanzie adeguate ai sensi dell'articolo 46, paragrafo 1, e dell'articolo 46, paragrafo 2, lettera c), del regolamento (UE) 2016/679 ai fini del trasferimento da un titolare del trattamento o un responsabile del trattamento di dati personali trattati soggetti a tale regolamento (esportatore) a un titolare del trattamento o un (sub-)responsabile del trattamento il cui trattamento di dati non è soggetto tale regolamento (importatore).

2. Le clausole contrattuali tipo stabiliscono inoltre i diritti e gli obblighi dei titolari del trattamento e dei responsabili del trattamento in relazione alle questioni di cui all'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 per quanto riguarda il trasferimento di dati personali da un titolare del trattamento a un responsabile del trattamento o da un responsabile del trattamento a un sub-responsabile del trattamento.

([12]) Parere congiunto 2/2021 dell'EDPB e del GEPD sulla decisione di esecuzione della Commissione europea relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi riguardo alle questioni di cui all'articolo 46, paragrafo 2, lettera c), del regolamento (UE) 2016/679

Articolo 2

Qualora l'importatore sia o sia diventato soggetto a una legislazione o prassi del paese terzo di destinazione che gli impedisce di rispettare le clausole contrattuali tipo figuranti in allegato e, di conseguenza, le autorità competenti dello Stato membro esercitino i poteri correttivi di cui all'articolo 58 del regolamento (UE) 2016/679 per sospendere o vietare i trasferimenti di dati verso paesi terzi, lo Stato membro interessato informa senza indugio la Commissione, che trasmette l'informazione agli altri Stati membri.

Articolo 3

La Commissione valuta l'applicazione pratica delle clausole contrattuali tipo figuranti in allegato, sulla base di tutte le informazioni disponibili, nell'ambito della valutazione periodica prevista all'articolo 97 del regolamento (UE) 2016/679.

Articolo 4

1. La presente decisione entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

2. La decisione 2001/497/CE è abrogata con effetto a decorrere dal 27 settembre 2021.

3. La decisione 2010/87/UE è abrogata con effetto a decorrere dal 27 settembre 2021.

4. I contratti conclusi prima del 27 settembre 2021 sulla base della decisione 2001/497/CE o della decisione 2010/87/UE sono ritenuti fornire garanzie adeguate ai sensi dell'articolo 46, paragrafo 1, del regolamento (UE) 2016/679 fino al 27 dicembre 2022, purché i trattamenti oggetto dei contratti rimangano invariati e il ricorso a tali clausole garantisca che il trasferimento di dati personali sia soggetto a garanzie adeguate.

Fatto a Bruxelles, il 4 giugno 2021

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO

CLAUSOLE CONTRATTUALI TIPO

SEZIONE I

Clausola 1

Scopo e ambito di applicazione

a) Scopo delle presenti clausole contrattuali tipo è garantire il rispetto dei requisiti del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) ([1]) in caso di trasferimento di dati personali verso un paese terzo.

b) Le parti:

i) la o le persone fisiche o giuridiche, la o le autorità pubbliche, lo o gli organismi o altri organi (di seguito la o le «entità») che trasferiscono i dati personali, elencate nell'allegato I.A. (di seguito «esportatore»), e

ii) la o le entità di un paese terzo che ricevono i dati personali dall'esportatore, direttamente o indirettamente tramite un'altra entità anch'essa parte delle presenti clausole, elencate nell'allegato I.A. (di seguito «importatore»)

hanno accettato le presenti clausole contrattuali tipo (di seguito «clausole»).

c) Le presenti clausole si applicano al trasferimento di dati personali specificato all'allegato I.B.

d) L'appendice delle presenti clausole contenente gli allegati ivi menzionati costituisce parte integrante delle presenti clausole.

Clausola 2

Effetto e invariabilità delle clausole

a) Le presenti clausole stabiliscono garanzie adeguate, compresi diritti azionabili degli interessati e mezzi di ricorso effettivi, in conformità dell'articolo 46, paragrafo 1, e dell'articolo 46, paragrafo 2, lettera c), del regolamento (UE) 2016/679 e, per quanto riguarda i trasferimenti di dati da titolari del trattamento a responsabili del trattamento e/o da responsabili del trattamento a responsabili del trattamento, clausole contrattuali tipo in conformità dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679, purché non siano modificate, tranne per selezionare il modulo o i moduli appropriati o per aggiungere o aggiornare informazioni nell'appendice. Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio e di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

b) Le presenti clausole non pregiudicano gli obblighi cui è soggetto l'esportatore a norma del regolamento (UE) 2016/679.

Clausola 3

Terzi beneficiari

a) Gli interessati possono invocare e far valere le presenti clausole, in qualità di terzi beneficiari, nei confronti dell'esportatore e/o dell'importatore, con le seguenti eccezioni:

i) clausola 1, clausola 2, clausola 3, clausola 6, clausola 7;

([1]) Qualora l'esportatore sia un responsabile del trattamento soggetto al regolamento (UE) 2016/679 che agisce per conto di un'istituzione o di un organo dell'Unione in qualità di titolare del trattamento, l'utilizzo delle presenti clausole quando è fatto ricorso a un altro responsabile del trattamento (sub-responsabile del trattamento) non soggetto al regolamento (UE) 2016/679 garantisce anche il rispetto dell'articolo 29, paragrafo 4, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39), nella misura in cui le presenti clausole e gli obblighi in materia di protezione dei dati stabiliti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento in conformità dell'articolo 29, paragrafo 3, del regolamento (UE) 2018/1725 sono allineati. Si tratta, in particolare, del caso in cui il titolare del trattamento e il responsabile del trattamento si basano sulle clausole contrattuali tipo incluse nella decisione 2021/915.

ii) clausola 8 - modulo uno: clausola 8.5, lettera e), e clausola 8.9, lettera b); modulo due: clausola 8.1, lettera b), clausola 8.9, lettere a), c), d) ed e); modulo tre: clausola 8.1, lettere a), c) e d), e clausola 8.9, lettere a), c), d), e), f) e g); modulo quattro: clausola 8.1, lettera b), e clausola 8.3, lettera b);

iii) clausola 9 - modulo due: clausola 9, lettere a), c), d) ed e); modulo tre: clausola 9, lettere a), c), d) ed e);

iv) clausola 12 - modulo uno: clausola 12, lettere a) e d); moduli due e tre: clausola 12, lettere a), d) e f);

v) clausola 13;

vi) clausola 15.1, lettere c), d) ed e);

vii) clausola 16, lettera e);

viii) clausola 18 - moduli uno, due e tre: clausola 18, lettere a) e b); modulo quattro: clausola 18.

b) La lettera a) lascia impregiudicati i diritti degli interessati a norma del regolamento (UE) 2016/679.

Clausola 4

Interpretazione

a) Quando le presenti clausole utilizzano termini che sono definiti nel regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui a detto regolamento.

b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679.

c) Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679.

Clausola 5

Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

Clausola 6

Descrizione dei trasferimenti

I dettagli dei trasferimenti, in particolare le categorie di dati personali trasferiti e le finalità per le quali i dati sono trasferiti, sono specificati nell'allegato I.B.

Clausola 7 — Facoltativa

Clausola di adesione successiva

a) Un'entità che non sia parte delle presenti clausole può, con l'accordo delle parti, aderire alle presenti clausole in qualunque momento, in qualità di esportatore o di importatore, compilando l'appendice e firmando l'allegato I.A.

b) Una volta compilata l'appendice e firmato l'allegato I.A, l'entità aderente diventa parte delle presenti clausole e ha i diritti e gli obblighi di un esportatore o di un importatore, conformemente alla sua designazione nell'allegato I.A.

c) L'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II — OBBLIGHI DELLE PARTI

Clausola 8

Garanzie in materia di protezione dei dati

L'esportatore garantisce di aver fatto quanto ragionevolmente possibile per stabilire che l'importatore, grazie all'attuazione di misure tecniche e organizzative adeguate, è in grado di adempiere agli obblighi che gli incombono a norma delle presenti clausole.

MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento

8.1. **Limitazione delle finalità**

L'importatore tratta i dati personali soltanto per le finalità specifiche del trasferimento di cui all'allegato I.B. Può trattare i dati personali per un'altra finalità soltanto:

i) se ha ottenuto il consenso preliminare dell'interessato;

ii) se il trattamento è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria nell'ambito di specifici procedimenti amministrativi, regolamentari o giudiziari; o

iii) se il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.

8.2. **Trasparenza**

a) Per consentire agli interessati di esercitare effettivamente i propri diritti in conformità della clausola 10, l'importatore li informa, direttamente o tramite l'esportatore, circa:

i) la sua identità e i suoi dati di contatto;

ii) le categorie di dati personali trattati;

iii) il diritto di ottenere una copia delle presenti clausole;

iv) qualora intenda trasferire successivamente i dati personali a terzi, il destinatario o le categorie di destinatari (ove opportuno al fine di fornire informazioni significative), la finalità del trasferimento successivo e il motivo dello stesso in conformità della clausola 8.7.

b) La lettera a) non si applica se l'interessato dispone già delle informazioni, anche quando tali informazioni sono già state fornite dall'esportatore, o se la comunicazione delle informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato per l'importatore. In quest'ultimo caso l'importatore, per quanto possibile, rende pubbliche le informazioni.

c) Su richiesta, le parti mettono gratuitamente a disposizione dell'interessato una copia delle presenti clausole, compresa l'appendice da loro compilata. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, le parti possono espungere informazioni dall'appendice prima di trasmetterne una copia, fornendo tuttavia una sintesi significativa qualora l'interessato non sia altrimenti in grado di comprenderne il contenuto o di esercitare i propri diritti. Su richiesta, le parti comunicano all'interessato le ragioni delle espunzioni, per quanto possibile senza rivelare le informazioni espunte.

d) Le lettere da a) a c) lasciano impregiudicati gli obblighi incombenti all'esportatore a norma degli articoli 13 e 14 del regolamento (UE) 2016/679.

8.3. **Esattezza e minimizzazione dei dati**

a) Ciascuna parte provvede affinché i dati personali siano esatti e, se necessario, aggiornati. L'importatore adotta tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

b) Se una parte viene a conoscenza del fatto che i dati personali che ha trasferito o ricevuto sono inesatti o obsoleti, ne informa senza ingiustificato ritardo l'altra parte.

c) L'importatore provvede affinché i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

8.4. **Limitazione della conservazione**

L'importatore conserva i dati personali per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono trattati. Mette in atto misure tecniche o organizzative adeguate per garantire il rispetto di tale obbligo, compresa la cancellazione o l'anonimizzazione ([2]) dei dati e di tutti i backup alla fine del periodo di conservazione.

8.5. **Sicurezza del trattamento**

a) L'importatore e, durante la trasmissione, anche l'esportatore mettono in atto misure tecniche e organizzative adeguate per garantire la sicurezza dei dati personali, compresa la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a tali dati (di seguito «violazione dei dati personali»). Nel valutare l'adeguato livello di sicurezza, essi tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi derivanti dal trattamento per gli interessati. Le parti prendono in considerazione in particolare la possibilità di ricorrere alla cifratura o alla pseudonimizzazione, anche durante la trasmissione, qualora la finalità del trattamento possa essere conseguita in tal modo.

b) Le parti concordano le misure tecniche e organizzative di cui all'allegato II. L'importatore effettua controlli regolari per garantire che tali misure continuino a offrire un adeguato livello di sicurezza.

c) L'importatore garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

d) In caso di una violazione dei dati personali trattati dall'importatore a norma delle presenti clausole, l'importatore adotta misure adeguate per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

e) In caso di una violazione dei dati personali che possa presentare un rischio per i diritti e le libertà delle persone fisiche, l'importatore informa l'esportatore e l'autorità di controllo competente in conformità della clausola 13 senza ingiustificato ritardo. Tale notifica contiene i) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati personali in questione), ii) le sue probabili conseguenze, iii) le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e iv) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni. Nella misura in cui non gli sia possibile fornire le informazioni contestualmente, l'importatore può fornirle in fasi successive senza ulteriore ingiustificato ritardo.

f) In caso di una violazione dei dati personali che possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'importatore informa senza ingiustificato ritardo gli interessati della violazione dei dati personali e della sua natura, se necessario in cooperazione con l'esportatore, unitamente alle informazioni di cui alla lettera e), punti da ii) a iv), a meno che l'importatore abbia attuato misure volte a ridurre in modo significativo il rischio per i diritti o le libertà delle persone fisiche o che la notifica implichi uno sforzo sproporzionato. In quest'ultimo caso, l'importatore effettua una comunicazione pubblica o adotta misure analoghe per informare il pubblico della violazione dei dati personali.

g) L'importatore documenta tutte le circostanze pertinenti relative alla violazione dei dati personali, comprese le sue conseguenze e i provvedimenti adottati per porvi rimedio, e ne tiene un registro.

8.6. **Dati sensibili**

Qualora il trasferimento riguardi dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati (in prosieguo «dati sensibili»), l'importatore applica limitazioni specifiche e/o garanzie supplementari adeguate alla natura specifica dei dati e ai rischi connessi. Ciò può includere limitazioni del personale autorizzato ad accedere ai dati personali, misure di sicurezza supplementari (quali la pseudonimizzazione) e/o limitazioni aggiuntive all'ulteriore divulgazione.

([2]) Questo richiede di rendere anonimi i dati in modo tale che la persona non sia più identificabile da nessuno, in linea con il considerando 26 del regolamento (UE) 2016/679, e che tale processo sia irreversibile.

8.7. **Trasferimenti successivi**

L'importatore non comunica i dati personali a terzi situati al di fuori dell'Unione europea ([3]) (nel suo stesso paese o in un altro paese terzo - di seguito: «trasferimento successivo»), a meno che il terzo sia o accetti di essere vincolato dalle presenti clausole, secondo il modulo appropriato. Altrimenti, il trasferimento successivo da parte dell'importatore può aver luogo solo se:

i) è diretto verso un paese che beneficia di una decisione di adeguatezza in conformità dell'articolo 45 del regolamento (UE) 2016/679 che copre il trasferimento successivo;

ii) il terzo fornisce in altro modo garanzie adeguate in conformità dell'articolo 46 o 47 del regolamento (UE) 2016/679 in relazione al trattamento in questione;

iii) il terzo stipula uno strumento vincolante con l'importatore che garantisce lo stesso livello di protezione dei dati previsto dalle presenti clausole e l'importatore fornisce una copia di tali garanzie all'esportatore;

iv) il trasferimento è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria nell'ambito di specifici procedimenti amministrativi, regolamentari o giudiziari;

v) il trasferimento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, o

vi) qualora non ricorra nessuna delle altre condizioni, l'importatore ha ottenuto il consenso esplicito dell'interessato al trasferimento successivo in una situazione specifica, dopo averlo informato delle sue finalità, dell'identità del destinatario e dei possibili rischi di siffatto trasferimento per l'interessato dovuti alla mancanza di garanzie adeguate in materia di protezione dei dati. In tal caso, l'importatore informa l'esportatore e, su richiesta di quest'ultimo, gli trasmette copia delle informazioni fornite all'interessato.

Qualunque trasferimento successivo è soggetto al rispetto da parte dell'importatore di tutte le altre garanzie previste dalle presenti clausole, in particolare la limitazione delle finalità.

8.8. **Trattamento sotto l'autorità dell'importatore**

L'importatore provvede affinché chiunque agisca sotto la sua autorità, compreso un responsabile del trattamento, tratti i dati soltanto su sua istruzione.

8.9. **Documentazione e rispetto**

a) Ciascuna parte deve essere in grado di dimostrare il rispetto degli obblighi che le incombono a norma delle presenti clausole. In particolare, l'importatore conserva documentazione adeguata delle attività di trattamento effettuate sotto la sua responsabilità.

b) Su richiesta, l'importatore mette tale documentazione a disposizione dell'autorità di controllo competente.

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

8.1. **Istruzioni**

a) L'importatore tratta i dati personali soltanto su istruzione documentata dell'esportatore. L'esportatore può impartire tali istruzioni per tutta la durata del contratto.

b) L'importatore informa immediatamente l'esportatore qualora non sia in grado di seguire tali istruzioni.

8.2. **Limitazione delle finalità**

L'importatore tratta i dati personali soltanto per le finalità specifiche del trasferimento di cui all'allegato I.B, salvo ulteriori istruzioni dell'esportatore.

([3]) L'accordo sullo Spazio economico europeo (accordo SEE) prevede l'estensione del mercato interno dell'Unione europea ai tre Stati del SEE: Islanda, Liechtenstein e Norvegia. La legislazione dell'Unione sulla protezione dei dati, regolamento (UE) 2016/679 compreso, è materia contemplata dall'accordo SEE, nel cui allegato XI è stata integrata. Pertanto, qualunque comunicazione da parte dell'importatore a terzi situati nel SEE non può essere considerata un trasferimento successivo ai fini delle presenti clausole.

8.3. **Trasparenza**

Su richiesta, l'esportatore mette gratuitamente a disposizione dell'interessato una copia delle presenti clausole, compresa l'appendice compilata dalle parti. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, comprese le misure descritte nell'allegato II e i dati personali, l'esportatore può espungere informazioni dall'appendice delle presenti clausole prima di trasmetterne una copia, fornendo tuttavia una sintesi significativa qualora l'interessato non sia altrimenti in grado di comprenderne il contenuto o di esercitare i propri diritti. Su richiesta, le parti comunicano all'interessato le ragioni delle espunzioni, per quanto possibile senza rivelare le informazioni espunte. Questa clausola lascia impregiudicati gli obblighi incombenti all'esportatore a norma degli articoli 13 e 14 del regolamento (UE) 2016/679.

8.4. **Esattezza**

Se l'importatore viene a conoscenza del fatto che i dati personali che ha ricevuto sono inesatti o obsoleti, ne informa senza ingiustificato ritardo l'esportatore. In tal caso, l'importatore coopera con l'esportatore per cancellarli o rettificarli.

8.5. **Durata del trattamento e cancellazione o restituzione dei dati**

L'importatore tratta i dati personali soltanto per la durata specificata nell'allegato I.B. Al termine della prestazione dei servizi di trattamento l'importatore, a scelta dell'esportatore, cancella tutti i dati personali trattati per conto dell'esportatore e certifica a quest'ultimo di averlo fatto, oppure restituisce all'esportatore tutti i dati personali trattati per suo conto e cancella le copie esistenti. Finché i dati non sono cancellati o restituiti, l'importatore continua ad assicurare il rispetto delle presenti clausole. Qualora la legislazione locale applicabile all'importatore vieti la restituzione o la cancellazione dei dati personali, l'importatore garantisce che continuerà ad assicurare il rispetto delle presenti clausole e che tratterà i dati solo nella misura e per il tempo richiesto dalla legislazione locale. Ciò lascia impregiudicata la clausola 14, in particolare il requisito per l'importatore, a norma della clausola 14, lettera e), di informare l'esportatore per tutta la durata del contratto se ha motivo di ritenere di essere, o essere diventato, soggetto a una legislazione o prassi non conformi ai requisiti di cui alla clausola 14, lettera a).

8.6. **Sicurezza del trattamento**

a) L'importatore e, durante la trasmissione, anche l'esportatore mettono in atto misure tecniche e organizzative adeguate per garantire la sicurezza dei dati, compresa la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a tali dati (di seguito «violazione dei dati personali»). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi derivanti dal trattamento per gli interessati. Le parti prendono in considerazione in particolare la possibilità di ricorrere alla cifratura o alla pseudonimizzazione, anche durante la trasmissione, qualora la finalità del trattamento possa essere conseguita in tal modo. In caso di pseudonimizzazione, le informazioni aggiuntive per l'attribuzione dei dati personali a un interessato specifico restano, ove possibile, sotto il controllo esclusivo dell'esportatore. Nell'adempiere all'obbligo ai sensi del presente paragrafo, l'importatore mette in atto almeno le misure tecniche e organizzative specificate nell'allegato II. L'importatore effettua controlli regolari per garantire che tali misure continuino a offrire un adeguato livello di sicurezza.

b) L'importatore concede l'accesso ai dati personali ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

c) In caso di violazione dei dati personali trattati dall'importatore a norma delle presenti clausole, l'importatore adotta misure adeguate per porre rimedio alla violazione, anche per attenuarne gli effetti negativi. L'importatore informa l'esportatore senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. Tale notifica contiene i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni, una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati personali in questione), le sue probabili conseguenze e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, se del caso anche per attenuarne i possibili effetti negativi. Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo;

d) L'importatore coopera con l'esportatore e lo assiste per consentirgli di adempiere agli obblighi che gli incombono a norma del regolamento (UE) 2016/679, in particolare di dare notifica all'autorità di controllo competente e agli interessati in questione, tenuto conto della natura del trattamento e delle informazioni di cui dispone l'importatore.

8.7. **Dati sensibili**

Qualora il trasferimento riguardi dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati (in prosieguo «dati sensibili»), l'importatore applica le limitazioni specifiche e/o le garanzie supplementari di cui all'allegato I.B.

8.8. **Trasferimenti successivi**

L'importatore comunica i dati personali a terzi soltanto su istruzione documentata dell'esportatore. L'importatore non comunica i dati personali a terzi situati al di fuori dell'Unione europea ([4]) (nel suo stesso paese o in un altro paese terzo - di seguito: «trasferimento successivo»), a meno che il terzo sia o accetti di essere vincolato dalle presenti clausole, secondo il modulo appropriato.

i) il trasferimento successivo è diretto verso un paese che beneficia di una decisione di adeguatezza in conformità dell'articolo 45 del regolamento (UE) 2016/679 che copre il trasferimento successivo;

ii) il terzo fornisce in altro modo garanzie adeguate in conformità dell'articolo 46 o 47 del regolamento (UE) 2016/679 in relazione al trattamento in questione;

iii) il trasferimento successivo è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria nell'ambito di specifici procedimenti amministrativi, regolamentari o giudiziari; o

iv) il trasferimento successivo è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.

Qualunque trasferimento successivo è soggetto al rispetto da parte dell'importatore di tutte le altre garanzie previste dalle presenti clausole, in particolare la limitazione delle finalità.

8.9. **Documentazione e rispetto**

a) L'importatore risponde prontamente e adeguatamente alle richieste di informazioni dell'esportatore relative al trattamento a norma delle presenti clausole.

b) Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole. In particolare, l'importatore conserva documentazione adeguata delle attività di trattamento effettuate per conto dell'esportatore.

c) L'importatore mette a disposizione dell'esportatore tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alle presenti clausole e, su richiesta dell'esportatore, consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, l'esportatore può tenere conto delle pertinenti certificazioni in possesso dell'importatore.

d) L'esportatore può scegliere di condurre l'attività di revisione autonomamente o di incaricare un revisore indipendente. Le attività di revisione possono comprendere ispezioni nei locali o nelle strutture fisiche dell'importatore e, se del caso, sono effettuate con un preavviso ragionevole.

e) Le parti mettono a disposizione dell'autorità di controllo competente, su richiesta, le informazioni di cui alle lettere b) e c), compresi i risultati di eventuali attività di revisione.

([4]) L'accordo sullo Spazio economico europeo (accordo SEE) prevede l'estensione del mercato interno dell'Unione europea ai tre Stati del SEE: Islanda, Liechtenstein e Norvegia. La legislazione dell'Unione sulla protezione dei dati, regolamento (UE) 2016/679 compreso, è materia contemplata dall'accordo SEE, nel cui allegato XI è stata integrata. Pertanto, qualunque comunicazione da parte dell'importatore a terzi situati nel SEE non può essere considerata un trasferimento successivo ai fini delle presenti clausole.

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

8.1. **Istruzioni**

a) L'esportatore informa l'importatore del fatto che agisce in qualità di responsabile del trattamento seguendo le istruzioni del o dei titolari del trattamento, che mette a disposizione dell'importatore prima del trattamento.

b) L'importatore tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, quale comunicatagli dall'esportatore, e su qualunque istruzione documentata aggiuntiva dell'esportatore. Tali istruzioni aggiuntive non devono essere in contrasto con le istruzioni del titolare del trattamento. Il titolare del trattamento o l'esportatore può impartire ulteriori istruzioni documentate in merito al trattamento dei dati per tutta la durata del contratto.

c) L'importatore informa immediatamente l'esportatore qualora non sia in grado di seguire tali istruzioni. Qualora l'importatore non sia in grado di seguire le istruzioni del titolare del trattamento, l'esportatore ne dà immediatamente notifica al titolare del trattamento.

d) L'esportatore garantisce di aver imposto all'importatore gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico a norma del diritto dell'Unione o degli Stati membri tra il titolare del trattamento e l'esportatore ([5]).

8.2. **Limitazione delle finalità**

L'importatore tratta i dati personali soltanto per le finalità specifiche del trasferimento di cui all'allegato I.B, salvo ulteriori istruzioni del titolare del trattamento, quali comunicategli dall'esportatore, o dell'esportatore.

8.3. **Trasparenza**

Su richiesta, l'esportatore mette gratuitamente a disposizione dell'interessato una copia delle presenti clausole, compresa l'appendice compilata dalle parti. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, le parti possono espungere informazioni dall'appendice prima di trasmetterne una copia, fornendo tuttavia una sintesi significativa qualora l'interessato non sia altrimenti in grado di comprenderne il contenuto o di esercitare i propri diritti. Su richiesta, le parti comunicano all'interessato le ragioni delle espunzioni, per quanto possibile senza rivelare le informazioni espunte.

8.4. **Esattezza**

Se l'importatore viene a conoscenza del fatto che i dati personali che ha ricevuto sono inesatti o obsoleti, ne informa senza ingiustificato ritardo l'esportatore. In tal caso, l'importatore coopera con l'esportatore per rettificarli o cancellarli.

8.5. **Durata del trattamento e cancellazione o restituzione dei dati**

L'importatore tratta i dati personali soltanto per la durata specificata nell'allegato I.B. Al termine della prestazione dei servizi di trattamento l'importatore, a scelta dell'esportatore, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica all'esportatore di averlo fatto, oppure restituisce all'esportatore tutti i dati personali trattati per suo conto e cancella le copie esistenti. Finché i dati non sono cancellati o restituiti, l'importatore continua ad assicurare il rispetto delle presenti clausole. Qualora la legislazione locale applicabile all'importatore vieti la restituzione o la cancellazione dei dati personali, l'importatore garantisce che continuerà ad assicurare il rispetto delle presenti clausole e che tratterà i dati solo nella misura e per il tempo richiesto dalla legislazione locale. Ciò lascia impregiudicata la clausola 14, in particolare il requisito per l'importatore, a norma della clausola 14, lettera e), di informare l'esportatore per tutta la durata del contratto se ha motivo di ritenere di essere, o essere diventato, soggetto a una legislazione o prassi non conformi ai requisiti di cui alla clausola 14, lettera a).

([5]) Cfr. l'articolo 28, paragrafo 4, del regolamento (UE) 2016/679 e, qualora il titolare del trattamento sia un'istituzione o un organo dell'UE, l'articolo 29, paragrafo 4, del regolamento (UE) 2018/1725.

8.6. **Sicurezza del trattamento**

a) L'importatore e, durante la trasmissione, anche l'esportatore mettono in atto misure tecniche e organizzative adeguate per garantire la sicurezza dei dati, compresa la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a tali dati (di seguito «violazione dei dati personali»). Nel valutare l'adeguato livello di sicurezza, essi tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi derivanti dal trattamento per gli interessati. Le parti prendono in considerazione in particolare la possibilità di ricorrere alla cifratura o alla pseudonimizzazione, anche durante la trasmissione, qualora la finalità del trattamento possa essere conseguita in tal modo. In caso di pseudonimizzazione, le informazioni aggiuntive per l'attribuzione dei dati personali a un interessato specifico restano, ove possibile, sotto il controllo esclusivo dell'esportatore o del titolare del trattamento. Nell'adempiere all'obbligo ai sensi del presente paragrafo, l'importatore mette in atto almeno le misure tecniche e organizzative specificate nell'allegato II. L'importatore effettua controlli regolari per garantire che tali misure continuino a offrire un adeguato livello di sicurezza.

b) L'importatore concede l'accesso ai dati ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

c) In caso di violazione dei dati personali trattati dall'importatore a norma delle presenti clausole, l'importatore adotta misure adeguate per porre rimedio alla violazione, anche per attenuarne gli effetti negativi. L'importatore informa l'esportatore e, ove opportuno e fattibile, il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. Tale notifica contiene i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni, una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati personali in questione), le sue probabili conseguenze e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi. Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo;

d) L'importatore coopera con l'esportatore e lo assiste per consentirgli di adempiere agli obblighi che gli incombono a norma del regolamento (UE) 2016/679, in particolare di dare notifica al titolare del trattamento affinché quest'ultimo possa a sua volta dare notifica all'autorità di controllo competente e agli interessati in questione, tenuto conto della natura del trattamento e delle informazioni di cui dispone l'importatore.

8.7. **Dati sensibili**

Qualora il trasferimento riguardi dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati (in prosieguo «dati sensibili»), l'importatore applica le limitazioni specifiche e/o le garanzie supplementari di cui all'allegato I.B.

8.8. **Trasferimenti successivi**

L'importatore comunica i dati personali a terzi soltanto su istruzione documentata del titolare del trattamento, quale comunicatagli dall'esportatore. L'importatore non comunica i dati personali a terzi situati al di fuori dell'Unione europea ([6]) (nel suo stesso paese o in un altro paese terzo - di seguito: «trasferimento successivo»), a meno che il terzo sia o accetti di essere vincolato dalle presenti clausole, secondo il modulo appropriato.

i) il trasferimento successivo è diretto verso un paese che beneficia di una decisione di adeguatezza in conformità dell'articolo 45 del regolamento (UE) 2016/679 che copre il trasferimento successivo;

([6]) L'accordo sullo Spazio economico europeo (accordo SEE) prevede l'estensione del mercato interno dell'Unione europea ai tre Stati del SEE: Islanda, Liechtenstein e Norvegia. La legislazione dell'Unione sulla protezione dei dati, regolamento (UE) 2016/679 compreso, è materia contemplata dall'accordo SEE, nel cui allegato XI è stata integrata. Pertanto, qualunque comunicazione da parte dell'importatore a terzi situati nel SEE non può essere considerata un trasferimento successivo ai fini delle presenti clausole.

ii) il terzo fornisce in altro modo garanzie adeguate in conformità dell'articolo 46 o 47 del regolamento (UE) 2016/679;

iii) il trasferimento successivo è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria nell'ambito di specifici procedimenti amministrativi, regolamentari o giudiziari; o

iv) il trasferimento successivo è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.

Qualunque trasferimento successivo è soggetto al rispetto da parte dell'importatore di tutte le altre garanzie previste dalle presenti clausole, in particolare la limitazione delle finalità.

8.9. **Documentazione e rispetto**

a) L'importatore risponde prontamente e adeguatamente alle richieste di informazioni dell'esportatore o del titolare del trattamento relative al trattamento a norma delle presenti clausole.

b) Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole. In particolare, l'importatore conserva documentazione adeguata delle attività di trattamento effettuate per conto del titolare del trattamento.

c) L'importatore mette tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alle presenti clausole a disposizione dell'esportatore, che le fornisce al titolare del trattamento.

d) L'importatore consente e contribuisce alle attività di revisione dell'esportatore delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Lo stesso vale qualora l'esportatore richieda che sia effettuata un'attività di revisione su istruzione del titolare del trattamento. Nel decidere in merito a un'attività di revisione, l'esportatore può tenere conto delle pertinenti certificazioni in possesso dell'importatore.

e) Qualora l'attività di revisione sia effettuata su istruzione del titolare del trattamento, l'esportatore ne mette i risultati a disposizione del titolare del trattamento.

f) L'esportatore può scegliere di condurre l'attività di revisione autonomamente o di incaricare un revisore indipendente. Le attività di revisione possono comprendere ispezioni nei locali o nelle strutture fisiche dell'importatore e, se del caso, sono effettuate con un preavviso ragionevole.

g) Le parti mettono a disposizione dell'autorità di controllo competente, su richiesta, le informazioni di cui alle lettere b) e c), compresi i risultati di eventuali attività di revisione.

MODULO QUATTRO: Trasferimento da responsabile del trattamento a titolare del trattamento

8.1. **Istruzioni**

a) L'esportatore tratta i dati personali soltanto su istruzione documentata dell'importatore, che agisce in qualità di titolare del trattamento.

b) L'esportatore informa immediatamente l'importatore qualora non sia in grado di seguire tali istruzioni, compreso qualora tali istruzioni violino il regolamento (UE) 2016/679 o altra legislazione dell'Unione o degli Stati membri in materia di protezione dei dati.

c) L'importatore si astiene da qualunque azione che impedisca all'esportatore di adempiere ai propri obblighi a norma del regolamento (UE) 2016/679, anche nel contesto di un sub-trattamento o per quanto riguarda la cooperazione con le autorità di controllo competenti.

d) Al termine della prestazione dei servizi di trattamento l'esportatore, a scelta dell'importatore, cancella tutti i dati personali trattati per conto dell'importatore e certifica a quest'ultimo di averlo fatto, oppure restituisce all'importatore tutti i dati personali trattati per suo conto e cancella le copie esistenti.

8.2. **Sicurezza del trattamento**

a) Le parti mettono in atto misure tecniche e organizzative adeguate per garantire la sicurezza dei dati, anche durante la trasmissione, e la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a tali dati (di seguito «violazione dei dati personali»). Nel valutare l'adeguato livello di sicurezza, tengono debitamente conto dello stato dell'arte, dei costi di attuazione, della natura dei dati personali ([7]), nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi derivanti dal trattamento per gli interessati e, in particolare, prendono in considerazione la possibilità di ricorrere alla cifratura o alla pseudonimizzazione, anche durante la trasmissione, qualora la finalità del trattamento possa essere conseguita in tal modo.

b) L'esportatore assiste l'importatore nel garantire un'adeguata sicurezza dei dati conformemente alla lettera a). In caso di violazione dei dati personali trattati dall'esportatore a norma delle presenti clausole, l'esportatore informa l'importatore senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione e assiste l'importatore nel porvi rimedio.

c) L'esportatore garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

8.3. **Documentazione e rispetto**

a) Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole.

b) L'esportatore mette a disposizione dell'importatore tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alle presenti clausole, e consente e contribuisce alle attività di revisione.

Clausola 9

Ricorso a sub-responsabili del trattamento

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

a) OPZIONE 1: AUTORIZZAZIONE PRELIMINARE SPECIFICA L'importatore non può subcontrattare a un sub-responsabile del trattamento le attività di trattamento da effettuare per conto dell'esportatore a norma delle presenti clausole senza la previa autorizzazione specifica scritta dell'esportatore. L'importatore presenta la richiesta di autorizzazione specifica almeno [*specificare il periodo*] prima di ricorrere al sub-responsabile del trattamento, unitamente alle informazioni necessarie per consentire all'esportatore di decidere in merito all'autorizzazione. L'elenco dei sub-responsabili del trattamento già autorizzati dall'esportatore figura nell'allegato III. Le parti tengono aggiornato tale allegato.

OPZIONE 2: AUTORIZZAZIONE SCRITTA GENERALE L'importatore ha l'autorizzazione generale dell'esportatore per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. L'importatore informa specificamente per iscritto l'esportatore di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno [*Specificare il periodo*], dando così all'esportatore tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento. L'importatore fornisce all'esportatore le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.

b) Qualora l'importatore ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto dell'esportatore), stipula un contratto scritto che prevede, nella sostanza, gli stessi obblighi in materia di protezione dei dati che vincolano l'importatore a norma delle presenti clausole, anche in termini di diritti del terzo beneficiario per gli interessati ([8]). Le parti convengono che, conformandosi alla presente clausola, l'importatore adempie agli obblighi di cui alla clausola 8.8. L'importatore garantisce che il sub-responsabile del trattamento rispetta gli obblighi cui l'importatore è soggetto in conformità delle presenti clausole.

([7]) Compreso il fatto che il trasferimento e l'ulteriore trattamento riguardino o meno dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati.

([8]) Questo requisito può essere soddisfatto dal sub-responsabile del trattamento che aderisce alle presenti clausole secondo il modulo appropriato, conformemente alla clausola 7.

c) Su richiesta dell'esportatore, l'importatore gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, l'importatore può espungere informazioni dal contratto prima di trasmetterne una copia.

d) L'importatore rimane pienamente responsabile nei confronti dell'esportatore dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con l'importatore. L'importatore notifica all'esportatore qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi derivanti da tale contratto.

e) L'importatore concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora l'importatore sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, l'esportatore ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

a) OPZIONE 1: AUTORIZZAZIONE PRELIMINARE SPECIFICA L'importatore non può subcontrattare a un sub-responsabile del trattamento le attività di trattamento da effettuare per conto dell'esportatore a norma delle presenti clausole senza la previa autorizzazione specifica scritta del titolare del trattamento. L'importatore presenta la richiesta di autorizzazione specifica almeno [*specificare il periodo*] prima di ricorrere al sub-responsabile del trattamento, unitamente alle informazioni necessarie per consentire al titolare del trattamento di decidere in merito all'autorizzazione. Informa l'esportatore di tale ricorso. L'elenco dei sub-responsabili del trattamento già autorizzati dal titolare del trattamento figura nell'allegato III. Le parti tengono aggiornato tale allegato.

OPZIONE 2: AUTORIZZAZIONE SCRITTA GENERALE L'importatore ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. L'importatore informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno [*Specificare il periodo*], dando così al titolare del trattamento tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento. L'importatore fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione. L'importatore informa l'esportatore del ricorso al o ai sub-responsabili del trattamento.

b) Qualora l'importatore ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento), stipula un contratto scritto che prevede, nella sostanza, gli stessi obblighi in materia di protezione dei dati che vincolano l'importatore a norma delle presenti clausole, anche in termini di diritti del terzo beneficiario per gli interessati ([9]). Le parti convengono che, conformandosi alla presente clausola, l'importatore adempie agli obblighi di cui alla clausola 8.8. L'importatore garantisce che il sub-responsabile del trattamento rispetta gli obblighi cui l'importatore è soggetto in conformità delle presenti clausole.

c) Su richiesta dell'esportatore o del titolare del trattamento, l'importatore fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, l'importatore può espungere informazioni dal contratto prima di trasmetterne una copia.

d) L'importatore rimane pienamente responsabile nei confronti dell'esportatore dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con l'importatore. L'importatore notifica all'esportatore qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi derivanti da tale contratto.

e) L'importatore concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora l'importatore sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, l'esportatore ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

([9]) Questo requisito può essere soddisfatto dal sub-responsabile del trattamento che aderisce alle presenti clausole secondo il modulo appropriato, conformemente alla clausola 7.

Clausola 10

Diritti dell'interessato

MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento

a) L'importatore, se del caso con l'assistenza dell'esportatore, tratta qualunque richiesta di informazioni e richiesta ricevute da un interessato in relazione al trattamento dei suoi dati personali e all'esercizio dei suoi diritti in virtù delle presenti clausole senza ingiustificato ritardo, al più tardi entro un mese dal ricevimento della richiesta di informazioni o richiesta ([10]). L'importatore adotta misure adeguate per agevolare tali richieste di informazioni, richieste e l'esercizio dei diritti dell'interessato. Tutte le informazioni fornite all'interessato sono in forma intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

b) In particolare, su richiesta dell'interessato, e gratuitamente, l'importatore:

   i) conferma all'interessato se i dati personali che lo riguardano sono o meno oggetto di trattamento e, in caso affermativo, fornisce una copia di tali dati e le informazioni di cui all'allegato I; se i dati personali sono stati o saranno oggetto di un trasferimento successivo, fornisce informazioni circa i destinatari o le categorie di destinatari (se del caso al fine di fornire informazioni significative) a cui i dati personali sono stati o saranno trasferiti, la finalità di tali trasferimenti successivi e il loro motivo in conformità della clausola 8.7; e fornisce informazioni sul diritto di proporre reclamo a un'autorità di controllo conformemente alla clausola 12, lettera c), punto i);

   ii) rettifica i dati inesatti o incompleti dell'interessato;

   iii) cancella i dati personali dell'interessato se tali dati sono o sono stati trattati in violazione di una delle presenti clausole, garantendo i diritti del terzo beneficiario, o se l'interessato revoca il consenso su cui si basa il trattamento.

c) Qualora l'importatore tratti i dati personali per finalità di marketing diretto, cessa il trattamento per tali finalità se l'interessato vi si oppone.

d) L'importatore non prende alcuna decisione basata unicamente sul trattamento automatizzato dei dati personali trasferiti (di seguito «decisione automatizzata»), che produca effetti giuridici che riguardano l'interessato o che incida in modo analogo significativamente sulla sua persona, salvo con il consenso esplicito dell'interessato o se autorizzato in tal senso dalla legislazione del paese di destinazione, a condizione che tale legislazione preveda misure adeguate a tutela dei diritti e dei legittimi interessi dell'interessato. In tal caso l'importatore, se necessario in cooperazione con l'esportatore:

   i) informa l'interessato della prevista decisione automatizzata, delle conseguenze previste e della logica utilizzata; e

   ii) attua garanzie adeguate, consentendo almeno all'interessato di contestare la decisione, esprimere la propria opinione e ottenere il riesame da parte di un essere umano.

e) Qualora le richieste dell'interessato siano eccessive, in particolare per il carattere ripetitivo, l'importatore può addebitare un contributo spese ragionevole tenuto conto dei costi amministrativi dell'accoglimento della richiesta o rifiutarsi di soddisfare la richiesta.

f) L'importatore può rifiutare la richiesta dell'interessato se tale rifiuto è consentito dalla legislazione del paese di destinazione ed è necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi di cui all'articolo 23, paragrafo 1, del regolamento (UE) 2016/679.

g) Se l'importatore intende rifiutare la richiesta dell'interessato, informa quest'ultimo dei motivi del rifiuto e della possibilità di proporre reclamo all'autorità di controllo competente e/o di proporre ricorso giurisdizionale.

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

a) L'importatore notifica prontamente all'esportatore qualunque richiesta ricevuta da un interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dall'esportatore.

([10]) Tale termine può essere prorogato al massimo di due mesi, se necessario, tenuto conto della complessità e del numero di richieste. L'importatore informa debitamente e prontamente l'interessato di tale proroga.

b) L'importatore assiste l'esportatore nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti in virtù del regolamento (UE) 2016/679. A tale riguardo, le parti stabiliscono nell'allegato II le misure tecniche e organizzative adeguate, tenuto conto della natura del trattamento, mediante le quali è fornita l'assistenza, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

c) Nell'adempiere agli obblighi di cui alle lettere a) e b), l'importatore si attiene alle istruzioni dell'esportatore.

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

a) L'importatore notifica prontamente all'esportatore e, se del caso, al titolare del trattamento qualunque richiesta ricevuta da un interessato, senza rispondere a tale richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

b) L'importatore assiste, se del caso in cooperazione con l'esportatore, il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti in virtù del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725, a seconda del caso. A tale riguardo, le parti stabiliscono nell'allegato II le misure tecniche e organizzative adeguate, tenuto conto della natura del trattamento, mediante le quali è fornita l'assistenza, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

c) Nell'adempiere agli obblighi di cui alle lettere a) e b), l'importatore si attiene alle istruzioni del titolare del trattamento comunicate dall'esportatore.

MODULO QUATTRO: Trasferimento da responsabile del trattamento a titolare del trattamento

Le parti dovrebbero prestarsi reciproca assistenza nel rispondere alle richieste di informazioni e alle richieste presentate dagli interessati a norma della legislazione locale applicabile all'importatore o, per il trattamento dei dati da parte dell'esportatore nell'UE, a norma del regolamento (UE) 2016/679.

Clausola 11

Ricorso

a) L'importatore informa gli interessati, in forma trasparente e facilmente accessibile, mediante avviso individuale o sul suo sito web, di un punto di contatto autorizzato a trattare i reclami. Tratta prontamente qualunque reclamo ricevuto da un interessato.

[OPZIONE: L'importatore accetta che gli interessati abbiano anche la possibilità di presentare gratuitamente reclamo a un organismo indipendente di risoluzione delle controversie ([11]). Informa gli interessati, secondo le modalità di cui alla lettera a), di tale meccanismo di ricorso e del fatto che non sono tenuti ad avvalersene o a seguire una particolare sequenza nel proporre ricorso.]

MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

b) In caso di controversia tra un interessato e una delle parti sul rispetto delle presenti clausole, la parte in questione fa tutto il possibile per risolvere la questione in via amichevole in modo tempestivo. Le parti si tengono reciprocamente informate di tali controversie e, se del caso, cooperano per risolverle.

c) Qualora l'interessato invochi un diritto del terzo beneficiario in conformità della clausola 3, l'importatore accetta la decisione dell'interessato di:

i) proporre reclamo all'autorità di controllo dello Stato membro di residenza abituale o del luogo di lavoro o all'autorità di controllo competente in conformità della clausola 13;

ii) deferire la controversia agli organi giurisdizionali competenti ai sensi della clausola 18.

([11]) L'importatore può offrire una risoluzione indipendente delle controversie tramite un organo arbitrale solo se è stabilito in un paese che ha ratificato la convenzione di New York sull'esecuzione dei lodi arbitrali.

d) Le parti accettano che l'interessato possa essere rappresentato da un organismo, un'organizzazione o un'associazione senza scopo di lucro alle condizioni di cui all'articolo 80, paragrafo 1, del regolamento (UE) 2016/679.

e) L'importatore si attiene a qualunque decisione vincolante a norma della legislazione applicabile dell'UE o degli Stati membri.

f) L'importatore dichiara che la scelta compiuta dall'interessato non pregiudica i diritti sostanziali o procedurali spettanti allo stesso relativamente ai rimedi giuridici previsti dalla legislazione applicabile.

Clausola 12

Responsabilità

MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento

MODULO QUATTRO: Trasferimento da responsabile del trattamento a titolare del trattamento

a) Ciascuna parte è responsabile nei confronti delle altre parti per i danni che essa ha causato loro violando le presenti clausole.

b) Ciascuna parte è responsabile nei confronti dell'interessato per i danni materiali o immateriali che essa gli ha causato violando i diritti del terzo beneficiario previsti dalle presenti clausole, e l'interessato ha il diritto di ottenere il risarcimento. Ciò lascia impregiudicata la responsabilità dell'esportatore a norma del regolamento (UE) 2016/679.

c) Qualora più di una parte sia responsabile per un danno causato all'interessato a seguito di una violazione delle presenti clausole, tutte le parti responsabili sono responsabili in solido e l'interessato ha il diritto di agire in giudizio contro una qualunque di loro.

d) Le parti convengono che, se una delle parti è ritenuta responsabile a norma della lettera c), essa ha il diritto di reclamare dalle altre parti la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno.

e) L'importatore non può invocare il comportamento di un responsabile del trattamento o un sub-responsabile del trattamento per sottrarsi alla propria responsabilità.

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

a) Ciascuna parte è responsabile nei confronti delle altre parti per i danni che essa ha causato loro violando le presenti clausole.

b) L'importatore è responsabile nei confronti dell'interessato per i danni materiali o immateriali che egli stesso o il suo sub-responsabile del trattamento ha causato all'interessato violando i diritti del terzo beneficiario riconosciuti dalle presenti clausole, e l'interessato ha il diritto di ottenere il risarcimento.

c) Nonostante la lettera b), l'esportatore è responsabile nei confronti dell'interessato per i danni materiali o immateriali che egli stesso o l'importatore (o il suo sub-responsabile del trattamento) ha causato all'interessato violando i diritti del terzo beneficiario riconosciuti dalle presenti clausole, e l'interessato ha il diritto di ottenere il risarcimento. Ciò lascia impregiudicata la responsabilità dell'esportatore e, qualora l'esportatore sia un responsabile del trattamento che agisce per conto di un titolare del trattamento, la responsabilità del titolare del trattamento a norma del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725, a seconda del caso.

d) Le parti convengono che, se l'esportatore è ritenuto responsabile a norma della lettera c) per i danni causati dall'importatore (o dal suo sub-responsabile del trattamento), egli ha il diritto di reclamare dall'importatore la parte del risarcimento corrispondente alla sua parte di responsabilità per il danno.

e) Qualora più di una parte sia responsabile per un danno causato all'interessato a seguito di una violazione delle presenti clausole, tutte le parti responsabili sono responsabili in solido e l'interessato ha il diritto di agire in giudizio contro una qualunque di loro.

f) Le parti convengono che, se una delle parti è ritenuta responsabile a norma della lettera e), essa ha il diritto di reclamare dalle altre parti la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno.

g) L'importatore non può invocare il comportamento di un sub-responsabile del trattamento per sottrarsi alla propria responsabilità.

Clausola 13

Controllo

MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

a) [Qualora l'esportatore sia stabilito in uno Stato membro dell'UE:] L'autorità di controllo responsabile di garantire che l'esportatore rispetti il regolamento (UE) 2016/679 per quanto riguarda il trasferimento dei dati, quale indicata all'allegato I.C, agisce in qualità di autorità di controllo competente.

[Qualora l'esportatore non sia stabilito in uno Stato membro dell'UE ma rientri nell'ambito di applicazione territoriale del regolamento (UE) 2016/679 conformemente all'articolo 3, paragrafo 2, di tale regolamento e abbia nominato un rappresentante in conformità dell'articolo 27, paragrafo 1, del medesimo regolamento:] L'autorità di controllo dello Stato membro in cui il rappresentante ai sensi dell'articolo 27, paragrafo 1, del regolamento (UE) 2016/679 è stabilito, quale indicata all'allegato I.C, agisce in qualità di autorità di controllo competente.

[Qualora l'esportatore non sia stabilito in uno Stato membro dell'UE ma rientri nell'ambito di applicazione territoriale del regolamento (UE) 2016/679 conformemente all'articolo 3, paragrafo 2, di tale regolamento e non abbia tuttavia nominato un rappresentante in conformità dell'articolo 27, paragrafo 2, del medesimo regolamento:] L'autorità di controllo di uno degli Stati membri in cui si trovano gli interessati i cui dati personali sono trasferiti a norma delle presenti clausole in relazione all'offerta di beni o alla prestazione di servizi, o il cui comportamento è oggetto di monitoraggio, quale indicata all'allegato I.C, agisce in qualità di autorità di controllo competente.

b) L'importatore accetta di sottoporsi alla giurisdizione dell'autorità di controllo competente e di cooperare con la stessa nell'ambito di qualunque procedura volta a garantire il rispetto delle presenti clausole. In particolare, l'importatore accetta di rispondere alle richieste di informazioni, sottoporsi ad attività di revisione e rispettare le misure adottate dall'autorità di controllo, comprese le misure di riparazione e risarcimento. Fornisce all'autorità di controllo conferma scritta che sono state adottate le misure necessarie.

SEZIONE III — LEGISLAZIONE E OBBLIGHI LOCALI IN CASO DI ACCESSO DA PARTE DI AUTORITÀ PUBBLICHE

Clausola 14

Legislazione e prassi locali che incidono sul rispetto delle clausole

MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

MODULO QUATTRO: Trasferimento da responsabile del trattamento a titolare del trattamento*(qualora il responsabile del trattamento stabilito nell'UE combini i dati personali ricevuti dal titolare del trattamento stabilito nel paese terzo con dati personali che ha raccolto nell'UE)*

a) Le parti garantiscono di non avere motivo di ritenere che la legislazione e le prassi del paese terzo di destinazione applicabili al trattamento dei dati personali da parte dell'importatore, compresi eventuali requisiti di comunicazione dei dati personali o misure che autorizzano l'accesso da parte delle autorità pubbliche, impediscono all'importatore di rispettare gli obblighi che gli incombono a norma delle presenti clausole. Ciò si basa sul presupposto che la legislazione e le prassi che rispettano l'essenza dei diritti e delle libertà fondamentali e non vanno oltre quanto necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi di cui all'articolo 23, paragrafo 1, del regolamento (UE) 2016/679 non sono in contraddizione con le presenti clausole.

b) Le parti dichiarano che, nel fornire la garanzia di cui alla lettera a), hanno tenuto debitamente conto dei seguenti elementi:

i) le circostanze specifiche del trasferimento, tra cui la lunghezza della catena di trattamento, il numero di attori coinvolti e i canali di trasmissione utilizzati; i trasferimenti successivi previsti; il tipo di destinatario; la finalità del trattamento; le categorie e il formato dei dati personali trasferiti; il settore economico in cui ha luogo il trasferimento; il luogo di conservazione dei dati trasferiti;

ii) la legislazione e le prassi del paese terzo di destinazione — comprese quelle che impongono la comunicazione di dati alle autorità pubbliche o che le autorizzano ad accedere ai dati — pertinenti alla luce delle circostanze specifiche del trasferimento, nonché le limitazioni e le garanzie applicabili ([12]);

iii) qualunque garanzia contrattuale, tecnica o organizzativa pertinente predisposta per integrare le garanzie di cui alle presenti clausole, comprese le misure applicate durante la trasmissione e il trattamento dei dati personali nel paese di destinazione.

c) L'importatore garantisce che, nell'effettuare la valutazione di cui alla lettera b), ha fatto tutto il possibile per fornire all'esportatore le informazioni pertinenti e dichiara che continuerà a cooperare con l'esportatore per garantire il rispetto delle presenti clausole.

d) Le parti accettano di documentare la valutazione di cui alla lettera b) e di metterla a disposizione dell'autorità di controllo competente su richiesta.

e) L'importatore accetta di informare prontamente l'esportatore se, dopo aver accettato le presenti clausole e per la durata del contratto, ha motivo di ritenere di essere, o essere diventato, soggetto a una legislazione o prassi non conformi ai requisiti di cui alla lettera a), anche a seguito di una modifica della legislazione del paese terzo o di una misura (ad esempio una richiesta di comunicazione) che indichi un'applicazione pratica di tale legislazione che non è conforme ai requisiti di cui alla lettera a). [Per il modulo tre: L'esportatore trasmette la notifica al titolare del trattamento.]

f) A seguito di una notifica in conformità della lettera e), o se ha altrimenti motivo di ritenere che l'importatore non sia più in grado di adempiere agli obblighi che gli incombono a norma delle presenti clausole, l'esportatore individua prontamente le misure adeguate (ad esempio, misure tecniche o organizzative per garantire la sicurezza e la riservatezza) che egli stesso e/o l'importatore devono adottare per far fronte alla situazione [per il modulo tre:, se del caso in consultazione con il titolare del trattamento]. L'esportatore sospende il trasferimento dei dati se ritiene che non possano essere assicurate garanzie adeguate per tale trasferimento, o su istruzione [per il modulo tre: del titolare del trattamento o] dell'autorità di controllo competente. In tal caso l'esportatore ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole. Se le parti del contratto sono più di due, l'esportatore può esercitare il diritto di risoluzione soltanto nei confronti della parte interessata, salvo diversamente concordato dalle parti. In caso di risoluzione del contratto in conformità della presente clausola, si applica la clausola 16, lettere d) ed e).

Clausola 15

Obblighi dell'importatore in caso di accesso da parte di autorità pubbliche

MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

MODULO QUATTRO: Trasferimento da responsabile del trattamento a titolare del trattamento*(qualora il responsabile del trattamento stabilito nell'UE combini i dati personali ricevuti dal titolare del trattamento stabilito nel paese terzo con dati personali che ha raccolto nell'UE)*

([12]) Per quanto riguarda l'impatto della legislazione e delle prassi sul rispetto delle presenti clausole, possono essere presi in considerazione diversi elementi nell'ambito di una valutazione globale. Tali elementi possono includere un'esperienza pratica pertinente e documentata in casi precedenti di richieste di comunicazione da parte di autorità pubbliche, o l'assenza di tali richieste, per un periodo di tempo sufficientemente rappresentativo. Si tratta in particolare di registri interni o altra documentazione, elaborati su base continuativa conformemente alla dovuta diligenza e certificati a livello di alta dirigenza, sempre che tali informazioni possano essere lecitamente condivise con terzi. Qualora per concludere che all'importatore non sarà impedito di rispettare le presenti clausole si faccia affidamento su questa esperienza pratica, essa deve essere sostenuta da altri elementi pertinenti e oggettivi, e spetta alle parti valutare attentamente se tali elementi, congiuntamente, abbiano un peso sufficiente in termini di affidabilità e rappresentatività per sostenere tale conclusione. In particolare, le parti devono considerare se la loro esperienza pratica è corroborata e non contraddetta da informazioni disponibili al pubblico, o altrimenti accessibili, e affidabili sull'esistenza o sull'assenza di richieste nello stesso settore e/o sull'applicazione pratica della legislazione, come la giurisprudenza e le relazioni di organi di vigilanza indipendenti.

15.1. **Notifica**

a) L'importatore accetta di informare prontamente l'esportatore e, ove possibile, l'interessato (se necessario con l'aiuto dell'esportatore) se:

i) riceve una richiesta giuridicamente vincolante di un'autorità pubblica, comprese le autorità giudiziarie, a norma della legislazione del paese di destinazione, di comunicare dati personali trasferiti in conformità delle presenti clausole; tale notifica comprende informazioni sui dati personali richiesti, sull'autorità richiedente, sulla base giuridica della richiesta e sulla risposta fornita; o

ii) viene a conoscenza di qualunque accesso diretto effettuato, conformemente alla legislazione del paese terzo di destinazione, da autorità pubbliche ai dati personali trasferiti in conformità delle presenti clausole; tale notifica comprende tutte le informazioni disponibili all'importatore.

[Per il modulo tre: L'esportatore trasmette la notifica al titolare del trattamento.]

b) Se la legislazione del paese di destinazione vieta all'importatore di informare l'esportatore e/o l'interessato, l'importatore accetta di fare tutto il possibile per ottenere un'esenzione dal divieto, al fine di comunicare al più presto quante più informazioni possibili. Per poterlo dimostrare su richiesta dell'esportatore, l'importatore accetta di documentare di aver fatto tutto il possibile.

c) Laddove consentito dalla legislazione del paese di destinazione, l'importatore accetta di fornire periodicamente all'esportatore, per la durata del contratto, quante più informazioni pertinenti possibili sulle richieste ricevute (in particolare, il numero di richieste, il tipo di dati richiesti, la o le autorità richiedenti, se le richieste sono state contestate e l'esito di tali contestazioni ecc.). [Per il modulo tre: L'esportatore trasmette le informazioni al titolare del trattamento.]

d) L'importatore accetta di conservare le informazioni di cui alle lettere da a) a c) per la durata del contratto e di metterle a disposizione dell'autorità di controllo competente su richiesta.

e) Le lettere da a) a c) lasciano impregiudicato l'obbligo dell'importatore in conformità della clausola 14, lettera e), e della clausola 16 di informare prontamente l'esportatore qualora non sia in grado di rispettare le presenti clausole.

15.2. **Riesame della legittimità e minimizzazione dei dati**

a) L'importatore accetta di riesaminare la legittimità della richiesta di comunicazione, in particolare il fatto che essa rientri o meno nei poteri conferiti all'autorità pubblica richiedente, e di contestarla qualora, dopo un'attenta valutazione, concluda che sussistono fondati motivi per ritenere che essa sia illegittima a norma della legislazione del paese di destinazione, compresi gli obblighi applicabili a norma del diritto internazionale e dei principi di cortesia internazionale. L'importatore, alle stesse condizioni, si avvale delle possibilità di ricorso. Quando contesta una richiesta, l'importatore chiede l'adozione di provvedimenti provvisori affinché gli effetti della richiesta siano sospesi fintantoché l'autorità giudiziaria competente non abbia deciso nel merito. Non comunica i dati personali richiesti fino a quando non sia tenuto a farlo ai sensi delle norme procedurali applicabili. Tali requisiti lasciano impregiudicati gli obblighi dell'importatore a norma della clausola 14, lettera e).

b) L'importatore accetta di documentare la propria valutazione giuridica e qualunque contestazione della richiesta di comunicazione e, nella misura consentita dalla legislazione del paese di destinazione, mette tale documentazione a disposizione dell'esportatore. Su richiesta, la mette a disposizione anche dell'autorità di controllo competente. [Per il modulo tre: L'esportatore mette la valutazione a disposizione del titolare del trattamento.]

c) Quando risponde a una richiesta di comunicazione l'importatore accetta di fornire la quantità minima di informazioni consentite, sulla base di un'interpretazione ragionevole della richiesta.

SEZIONE IV — DISPOSIZIONI FINALI

Clausola 16

Inosservanza delle clausole e risoluzione

a) L'importatore informa prontamente l'esportatore qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

b) Qualora l'importatore violi le presenti clausole o non sia in grado di rispettarle, l'esportatore sospende il trasferimento dei dati personali all'importatore fino a che il rispetto non sia nuovamente garantito o il contratto non sia risolto. Ciò lascia impregiudicata la clausola 14, lettera f).

c) L'esportatore ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora:

   i) l'esportatore abbia sospeso il trasferimento dei dati personali all'importatore in conformità della lettera b) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;

   ii) l'importatore violi in modo sostanziale o persistente le presenti clausole; o

   iii) l'importatore non si conformi a una decisione vincolante di un organo giurisdizionale competente o di un'autorità di controllo competente in merito agli obblighi che gli incombono a norma delle presenti clausole.

   In tali casi, informa l'autorità di controllo competente [per il modulo tre: e il titolare del trattamento] di tale inosservanza. Qualora le parti del contratto siano più di due, l'esportatore può esercitare il diritto di risoluzione soltanto nei confronti della parte interessata, salvo diversamente concordato dalle parti.

d) [Per i moduli uno, due e tre: I dati personali che sono stati trasferiti prima della risoluzione del contratto in conformità della lettera c) sono, a scelta dell'esportatore, restituiti immediatamente all'esportatore o cancellati integralmente. Lo stesso vale per qualunque copia dei dati.] [Per il modulo quattro: I dati personali raccolti dall'esportatore nell'UE che sono stati trasferiti prima della risoluzione del contratto in conformità della lettera c) sono cancellati immediatamente e integralmente, compresa qualunque loro copia. L'importatore certifica all'esportatore la cancellazione dei dati. Finché i dati non sono cancellati o restituiti, l'importatore continua ad assicurare il rispetto delle presenti clausole. Qualora la legislazione locale applicabile all'importatore vieti la restituzione o la cancellazione dei dati personali trasferiti, l'importatore garantisce che continuerà ad assicurare il rispetto delle presenti clausole e che tratterà i dati solo nella misura e per il tempo richiesto dalla legislazione locale.

e) Ciascuna parte può revocare il proprio accordo a essere vincolata dalle presenti clausole qualora i) la Commissione europea adotti una decisione in conformità dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 riguardante il trasferimento di dati personali cui si applicano le presenti clausole; o ii) il regolamento (UE) 2016/679 diventi parte del quadro giuridico del paese verso il quale i dati personali sono trasferiti. Ciò lascia impregiudicati gli altri obblighi che si applicano al trattamento in questione a norma del regolamento (UE) 2016/679.

Clausola 17

Legge applicabile

MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

[OPZIONE 1: Le presenti clausole sono disciplinate dalla legge di uno degli Stati membri dell'UE, purché essa riconosca i diritti del terzo beneficiario. Le parti convengono che tale legge è quella di _____ (*specificare lo Stato membro*).]

[OPZIONE 2 (per i moduli due e tre): Le presenti clausole sono disciplinate dalla legge dello Stato membro in cui è stabilito l'esportatore. Qualora tale legge non preveda i diritti del terzo beneficiario, questi sono disciplinati dalla legge di un altro Stato membro dell'UE che riconosce i diritti del terzo beneficiario. Le parti convengono che tale legge è quella di _____ (*specificare lo Stato membro*).]

MODULO QUATTRO: Trasferimento da responsabile del trattamento a titolare del trattamento

Le presenti clausole sono disciplinate dalla legge di un paese che riconosce i diritti del terzo beneficiario. Le parti convengono che tale legge è quella di _____ (*specificare il paese*).

Clausola 18

Scelta del foro e giurisdizione

MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

a) Qualunque controversia derivante dalle presenti clausole è risolta dagli organi giurisdizionali di uno Stato membro dell'UE.

b) Le parti convengono che tali organi giurisdizionali sono quelli di _____ (*specificare lo Stato membro*).]

c) L'interessato può agire in giudizio contro l'esportatore e/o l'importatore anche dinanzi agli organi giurisdizionali dello Stato membro in cui ha la propria residenza abituale.

d) Le parti accettano di sottoporsi alla giurisdizione di tali organi giurisdizionali.

MODULO QUATTRO: Trasferimento da responsabile del trattamento a titolare del trattamento

Qualunque controversia derivante dalle presenti clausole è risolta dagli organi giurisdizionali di _____ (*specificare il paese*).

APPENDICE

NOTA ESPLICATIVA:

Deve essere possibile distinguere chiaramente le informazioni applicabili a ciascun trasferimento o a ciascuna categoria di trasferimenti e, a tale riguardo, determinare i ruoli rispettivi delle parti quali esportatori e/o importatori. Non occorre per forza compilare e firmare appendici distinte per ciascun trasferimento/categoria di trasferimenti e/o rapporto contrattuale laddove tale trasparenza possa essere garantita con un'unica appendice. Tuttavia, ove necessario per assicurare una sufficiente chiarezza, dovrebbero essere utilizzate appendici distinte.

ALLEGATO I

A. **ELENCO DELLE PARTI**

MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

MODULO QUATTRO: Trasferimento da responsabile del trattamento a titolare del trattamento

Esportatore/i:*[Identità e dati di contatto del o degli esportatori e, se del caso, del suo/loro responsabile della protezione dei dati e/o rappresentante nell'Unione europea]*

1. Nome: ……

Indirizzo: ……

Nome, qualifica e dati di contatto del referente: ……

Attività pertinenti ai dati trasferiti a norma delle presenti clausole: ……

Firma e data: ……

Ruolo (titolare del trattamento/responsabile del trattamento): ……

2. ……

Importatore/i:*[Identità e dati di contatto del o degli importatori, compreso qualsiasi referente con responsabilità in materia di protezione dei dati]*

1. Nome: ……

Indirizzo: ……

Nome, qualifica e dati di contatto del referente: ……

Attività pertinenti ai dati trasferiti a norma delle presenti clausole: ……

Firma e data: ……

Ruolo (titolare del trattamento/responsabile del trattamento): ……

2. ……

B. **DESCRIZIONE DEL TRASFERIMENTO**

MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

MODULO QUATTRO: Trasferimento da responsabile del trattamento a titolare del trattamento

Categorie di interessati i cui dati personali sono trasferiti

……

Categorie di dati personali trasferiti

……

Dati sensibili trasferiti (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari.

……

La frequenza del trasferimento (ad esempio se i dati sono trasferiti come evento singolo o su base continua)

……

Natura del trattamento

……

Finalità del trasferimento dei dati e dell'ulteriore trattamento

……

Periodo di conservazione dei dati personali oppure, se non è possibile, criteri utilizzati per determinare tale periodo

……

Per i trasferimenti a (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento

……

C. **AUTORITÀ DI CONTROLLO COMPETENTE**

MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

Identificare la o le autorità di controllo competenti conformemente alla clausola 13

……

ALLEGATO II

MISURE TECNICHE E ORGANIZZATIVE, COMPRESE MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

NOTA ESPLICATIVA:

Le misure tecniche e organizzative devono essere descritte in termini specifici (e non generici). Si veda anche la nota esplicativa nella prima pagina dell'appendice, in particolare riguardo alla necessità di indicare chiaramente quali misure si applicano a ciascun trasferimento/insieme di trasferimenti.

Descrizione delle misure tecniche e organizzative messe in atto dal o dagli importatori (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.

[Esempi di possibili misure:

misure di pseudonimizzazione e cifratura dei dati personali

misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento

misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

misure di identificazione e autorizzazione dell'utente

misure di protezione dei dati durante la trasmissione

misure di protezione dei dati durante la conservazione

misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati

misure per garantire la registrazione degli eventi

misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita

misure di informatica interna e di gestione e governance della sicurezza informatica

misure di certificazione/garanzia di processi e prodotti

misure per garantire la minimizzazione dei dati

misure per garantire la qualità dei dati

misure per garantire la conservazione limitata dei dati

misure per garantire la responsabilità

misure per consentire la portabilità dei dati e garantire la cancellazione]

Per i trasferimenti a (sub-)responsabili del trattamento, descrivere anchele misure tecniche e organizzative specifiche che il (sub-) responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento e, per i trasferimenti da un responsabile del trattamento a un sub-responsabile del trattamento, all'esportatore

ALLEGATO III

ELENCO DEI SUB-RESPONSABILI DEL TRATTAMENTO

MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento

MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento

NOTA ESPLICATIVA:

Il presente allegato deve essere compilato per i moduli due e tre, in caso di autorizzazione specifica di sub-responsabili del trattamento (clausola 9, lettera a), opzione 1).

Il titolare del trattamento ha autorizzato il ricorso ai seguenti sub-responsabili del trattamento:

1. Nome: ……

   Indirizzo: ……

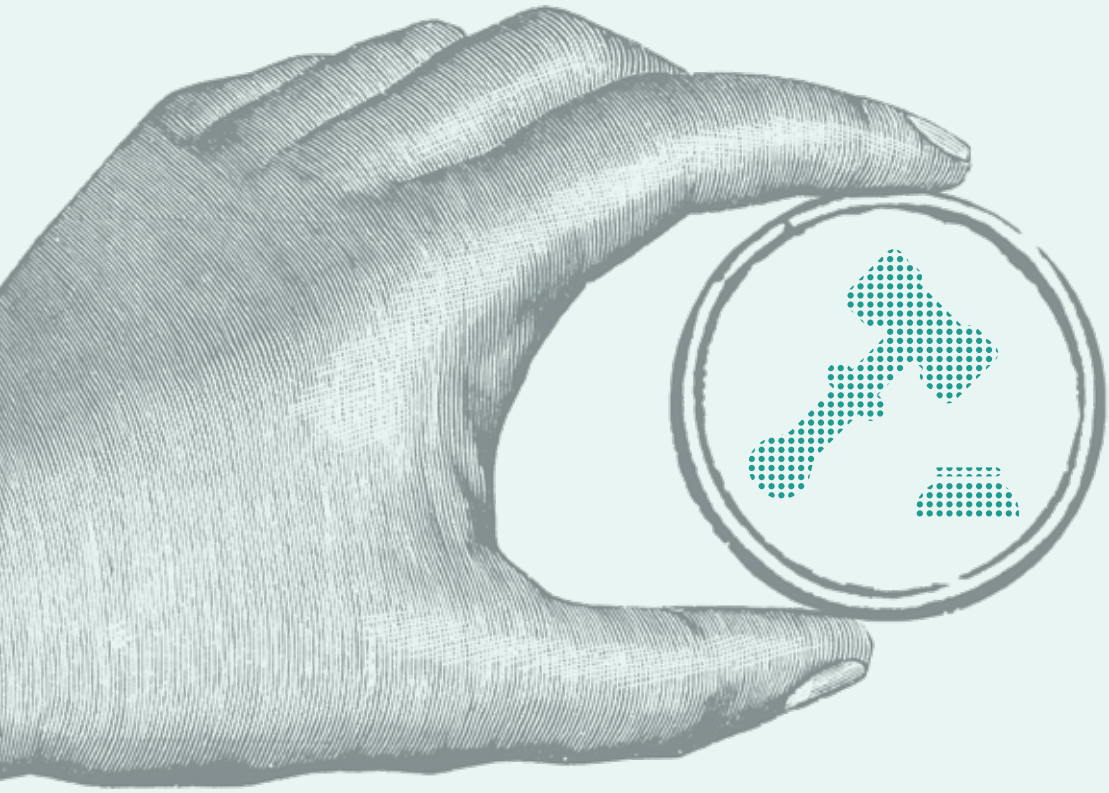
   Nome, qualifica e dati di contatto del referente: ……

   Descrizione del trattamento (compresa una chiara delimitazione delle responsabilità qualora siano autorizzati più sub-responsabili del trattamento): ……

2. ……

Torna a **Indice**

4 Meccanismi di applicazione del GDPR



Premessa
Meccanismi di applicazione del GDPR

Alcune delle novità più importanti del GDPR riguardano i meccanismi preposti alla sua applicazione da parte delle Autorità di controllo, come il Garante, incaricate di vigilarne l'osservanza.

Fra tali fondamentali innovazioni del GDPR vi è la previsione di un meccanismo di "sportello unico" per le imprese e le aziende che abbiano più stabilimenti nell'Ue nel contesto delle cui attività svolgano trattamenti di dati personali, o che offrano prodotti o servizi in più di un Paese dell'Ue a partire da un solo stabilimento in uno Stato membro. Lo sportello unico è l'Autorità di controllo dello Stato membro ove quel titolare o responsabile ha il proprio stabilimento unico o principale, e tale Autorità funge da interlocutore unico del titolare o del responsabile anche per tutti i reclami o i contenziosi che dovessero sorgere in altri Paesi dell'Ue; per questo viene definita "autorità capofila" e in questo senso è l'autorità che guida il processo di adozione della decisione relativa allo specifico trattamento transfrontaliero.

Proprio allo scopo di fornire ulteriori chiarimenti circa il funzionamento del meccanismo di sportello unico, il Comitato ha adottato un **parere (8/2019)** in merito alla definizione dei criteri che disciplinano la competenza dell'autorità capofila al mutare delle condizioni previste. Il parere chiarisce che la competenza ad agire in qualità di autorità capofila cambia al mutare delle condizioni relative allo stabilimento principale (che il titolare o responsabile dovrà dimostrare essere effettivamente tale) e che tale mutamento di competenze è ammesso fino al momento dell'adozione della decisione finale all'esito del procedimento di cooperazione ai sensi dell'art. 60 GDPR. L'autorità che ha svolto il ruolo di capofila precedentemente all'assunzione di tale decisione finale sarà quindi tenuta a condividere ogni informazione con la nuova autorità capofila in modo da consentire la più celere definizione del procedimento.

Un elemento essenziale all'interno della procedura di sportello unico al fine di assicurare il pieno coinvolgimento delle altre autorità interessate è la possibilità

di presentare obiezioni "pertinenti e motivate" al progetto di decisione dell'autorità capofila. Attraverso le **linee guida 9/2020**, il Comitato ha chiarito i profili sostanziali e procedurali in materia, analizzando sia i profili della pertinenza dell'obiezione rispetto alla materia trattata sia la necessità di un'adeguata motivazione e di un ragionamento chiaro e lineare; il presupposto di fondo è, tuttavia, che le autorità di controllo coinvolte (capofila e interessate) dovrebbero adoperarsi il più possibile per giungere ad un progetto di decisione consensuale anche attraverso un congruo scambio di informazioni a monte, facendo salvo pienamente il diritto al contraddittorio delle parti (titolare/responsabile, interessato) in conformità con il diritto nazionale rispettivamente applicabile. In questo senso, l'obiezione "pertinente e motivata" dovrebbe essere considerata come soluzione di ultima istanza, anche con riferimento all'analisi giuridica effettuata e all'ambito delle indagini svolte dall'autorità capofila sul caso in questione. In una prospettiva più generale, il Comitato ha ritenuto importante fornire chiarimenti anche sull'art. 3 del GDPR, relativo all'ambito di applicazione territoriale (**linee guida 3/2018**), che rappresenta una novità significativa rispetto al quadro normativo preesistente (direttiva 95/46/CE). L'art. 3 riflette l'intenzione del legislatore di assicurare un'ampia protezione dei diritti degli interessati nell'UE a fronte di trattamenti sempre più globalizzati e definisce l'ambito di applicazione del GDPR sulla base di specifici criteri. Le linee guida esaminano pertanto l'interpretazione di tali criteri: il criterio dello stabilimento, in base al quale il GDPR si applica al trattamento dei dati effettuati nell'ambito delle attività di uno stabilimento da parte di un titolare o di un responsabile del trattamento nell'UE, indipendentemente dal fatto che esso avvenga nell'UE; il criterio del *targeting*, una delle novità del nuovo quadro normativo, che rende applicabile il GDPR ai trattamenti di dati che, pur essendo effettuati da titolari non stabiliti nell'UE, sono relativi ad interessati che si trovano nell'Unione e riguardano l'offerta di beni o la prestazione di servizi agli stessi rivolti, o il monitoraggio del loro comportamento nel territorio UE; il criterio (classico) dell'applicazione del GDPR in virtù dei principi di diritto internazionale pubblico (ossia, ove un titolare sia stabilito in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico, come in ambasciate e consolati). Inoltre, poiché i titolari e i responsabili stabiliti fuori dall'UE i cui trattamenti rientrino nell'ambito di applicazione del GDPR sulla base del criterio del *targeting* sono tenuti a designare un rappresentante nell'Unione, le linee guida esaminano anche la procedura di tale designazione analizzando le responsabilità che da essa derivano e le deroghe previste in merito dal GDPR.

Torna a Indice | Premessa

Linee guida 3/2018 sull'ambito di applicazione territoriale del RGPD (articolo 3) Versione 2.1

12 novembre 2019

Cronologia delle versioni

Versione 2.1	7 gennaio 2020	Modifica di formattazione
Versione 2.0	12 novembre 2019	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	16 novembre 2018	Adozione delle linee guida ai fini della consultazione pubblica

Indice

Introduzione

1 Applicazione del criterio di stabilimento: articolo 3, paragrafo 1

2 Applicazione del criterio dell'indirizzamento (targeting) del trattamento (articolo 3, paragrafo 2)

3 Trattamento di dati in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico

4 Rappresentante di titolari o responsabili del trattamento non stabiliti nell'Unione

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

considerando l'articolo 70, paragrafo 1, lettera e), del regolamento 2016/679/UE del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

INTRODUZIONE

L'ambito di applicazione territoriale del regolamento generale sulla protezione dei dati[1] (il RGPD o il regolamento) è stabilito dall'articolo 3 del regolamento e rappresenta una significativa evoluzione della normativa dell'Unione europea sulla protezione dei dati rispetto al quadro definito dalla direttiva 95/46/CE.[2] In parte, il RGPD conferma le scelte operate dal legislatore dell'UE e dalla Corte di giustizia dell'Unione europea (CGUE) nel contesto della direttiva 95/46/CE. Tuttavia, nel regolamento sono state introdotte importanti novità. Ancor più importante è il fatto che, mentre il principale obiettivo dell'articolo 4 della direttiva era definire quale diritto nazionale di uno Stato membro fosse applicabile, l'articolo 3 del RGPD definisce l'ambito di applicazione territoriale di un atto normativo direttamente applicabile. Inoltre, mentre l'articolo 4 della direttiva fa riferimento a «strumenti» utilizzati sul territorio dell'Unione per ricondurre titolari del trattamento «non stabilit[i] nel territorio della Comunità» nell'ambito di applicazione della normativa sulla protezione dei dati dell'UE, tale riferimento non compare nell'articolo 3 del RGPD.

L'articolo 3 del RGPD rispecchia la volontà del legislatore di assicurare una tutela globale dei diritti degli interessati nell'UE e di stabilire, in termini di requisiti sulla protezione dei dati, una parità di condizioni per le imprese attive sui mercati UE, in un contesto caratterizzato da flussi di dati su scala mondiale.

L'articolo 3 del RGPD definisce l'ambito di applicazione territoriale del regolamento sulla base di due criteri principali: il criterio dello «stabilimento», di cui all'articolo 3, paragrafo 1, e il criterio dell'«indirizzamento (targeting)» del trattamento di cui all'articolo 3, paragrafo 2. Qualora sia soddisfatto uno di questi due criteri, il titolare o il responsabile del trattamento applicherà le disposizioni pertinenti del RGPD al trattamento di dati personali in questione. Inoltre, l'articolo 3, paragrafo 3, conferma l'applicazione del RGPD al trattamento nel caso in cui si applichi il diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Attraverso l'interpretazione condivisa da parte delle autorità di protezione dei dati nell'Unione europea, le presenti Linee guida intendono assicurare una coerente applicazione del RGPD nel valutare se un determinato trattamento svolto da un titolare o un responsabile rientri o meno nell'ambito di applicazione del nuovo quadro giuridico dell'UE. Nelle sue Linee guida, il comitato europeo per la protezione dei dati (CEPD) espone e chiarisce i criteri per determinare l'ambito di applicazione territoriale del RGPD. Tale interpretazione comune è altresì essenziale per i titolari e i responsabili del trattamento, sia all'interno sia al di fuori dell'UE, affinché possano valutare se siano tenuti a rispettare le disposizioni del RGPD per una determinata attività di trattamento.

Poiché i titolari o i responsabili del trattamento non stabiliti nell'UE, ma impegnati in attività di trattamento che rientrano nel campo di applicazione dell'articolo 3, paragrafo 2, sono tenuti a designare un rappresentante nell'Unione, le presenti Linee guida forniscono anche chiarimenti sul processo di designazione del rappresentante a norma dell'articolo 27, nonché sui rispettivi obblighi e responsabilità.

In linea generale il CEPD afferma che, laddove un trattamento di dati personali rientri nell'ambito di applicazione territoriale del RGPD, tutte le disposizioni del regolamento si applicano a tale trattamento. Le presenti Linee guida specificano i diversi scenari che potrebbero verificarsi, a seconda del tipo di trattamento, dei soggetti che lo realizzano o della collocazione geografica di tali soggetti, e indicano in dettaglio le disposizioni applicabili a ciascuna situazione. È pertanto essenziale che i titolari e i responsabili del trattamento, specie quelli che offrono beni e servizi a livello internazionale, effettuino un'attenta valutazione in concreto delle proprie attività di trattamento, al fine di determinare se il trattamento dei dati personali in questione rientri o meno nell'ambito di applicazione del RGPD.

Il CEPD sottolinea che l'articolo 3 mira a determinare se una specifica attività di trattamento, e non già una specifica persona (fisica o giuridica), rientri nell'ambito di applicazione del RGPD. Di conseguenza, talune attività di trattamento di dati personali da parte di un titolare o un responsabile potrebbero rientrare nell'ambito di applicazione del regolamento, mentre altre attività dello stesso titolare o responsabile potrebbero non rientrarvi, a seconda dello specifico trattamento.

Le presenti Linee guida, inizialmente adottate dal CEPD il 16 novembre, sono state sottoposte a consultazione pubblica dal 23 novembre 2018 al 18 gennaio 2019 e sono state successivamente aggiornate tenendo conto dei contributi e dei riscontri ricevuti.

1. APPLICAZIONE DEL CRITERIO DI STABILIMENTO: ARTICOLO 3, PARAGRAFO 1

L'articolo 3, paragrafo 1, del RGPD dispone che il «*regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*».

L'articolo 3, paragrafo 1, del RGPD fa riferimento non solo a uno stabilimento di un titolare del trattamento, ma anche a uno stabilimento di un responsabile del trattamento. Pertanto, anche il trattamento di dati personali da parte di un responsabile può essere soggetto al diritto dell'UE in virtù del fatto che tale responsabile del trattamento ha uno stabilimento all'interno dell'UE.

L'articolo 3, paragrafo 1, assicura che il RGPD si applichi al trattamento realizzato da un titolare o da un responsabile del trattamento nel contesto delle attività di uno stabilimento di tale titolare o responsabile all'interno dell'Unione, a prescindere dal luogo effettivo del trattamento. Il CEPD raccomanda pertanto un approccio tripartito al fine di determinare se un trattamento dei dati personali rientri o meno nell'ambito di applicazione del RGPD a norma dell'articolo 3, paragrafo 1.

Le sezioni seguenti chiariscono l'applicazione del criterio di stabilimento, in primo luogo considerando la definizione di «stabilimento» nell'UE ai sensi del

diritto dell'UE in materia di protezione dei dati, in secondo luogo esaminando ciò che si intende per «trattamento nell'ambito delle attività di uno stabilimento nell'Unione» e, infine, confermando che il RGPD si applica indipendentemente dal fatto che il trattamento effettuato nel contesto delle attività di tale stabilimento avvenga o meno nell'Unione.

a) «Uno stabilimento nell'Unione»

Prima di analizzare cosa si intenda per «uno stabilimento nell'Unione» occorre individuare chi è il titolare o il responsabile di una determinata attività di trattamento. Secondo la definizione di cui all'articolo 4, paragrafo 7, del RGPD, titolare del trattamento significa «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali». Un responsabile del trattamento, secondo l'articolo 4, paragrafo 8, del RGPD, è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento». Come stabilito dalla pertinente giurisprudenza della CGUE e dal precedente parere del Gruppo di lavoro "Articolo 29",[3] stabilire se un soggetto sia un titolare o un responsabile del trattamento ai fini del diritto dell'UE in materia di protezione dei dati è fondamentale per valutare l'applicazione del RGPD al trattamento dei dati personali in questione.

Sebbene la nozione di «stabilimento principale» sia definita nell'articolo 4, paragrafo 16, il RGPD non fornisce una definizione del concetto di «stabilimento» ai fini dell'articolo 3.[4] Tuttavia, il considerando 22[5] chiarisce che «*[l]o stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica*».

Questa formulazione è identica a quella del considerando 19 della direttiva 95/46/CE, cui è stato fatto riferimento in varie sentenze della CGUE che hanno ampliato l'interpretazione del termine «stabilimento», discostandosi da un'impostazione formalistica secondo cui un'impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata.[6] Di fatto, la CGUE ha stabilito che la nozione di «stabilimento» si estende a qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un'organizzazione stabile.[7] Al fine di determinare se un'entità con sede al di fuori dell'Unione abbia uno stabilimento in uno Stato membro, occorre valutare sia il grado di stabilità dell'organizzazione sia l'effettivo esercizio di attività in tale Stato membro alla luce della natura specifica delle attività economiche e della prestazione di servizi di cui trattasi. Ciò è particolarmente vero per le imprese che offrono servizi esclusivamente su Internet.[8]

In realtà, la soglia per configurare una «organizzazione stabile»[9] può essere piuttosto bassa quando le attività di un titolare del trattamento si focalizzano sulla prestazione di servizi online. Di conseguenza, in alcune circostanze la presenza nell'Unione di un solo dipendente o agente di un soggetto extra UE può essere sufficiente a configurare un'organizzazione stabile (equivalente a «stabilimento» ai fini dell'articolo 3, paragrafo 1) se l'attività di tale dipendente o agente è suffi-

cientemente stabile. Per contro, quando un dipendente è localizzato nell'UE, ma il trattamento non viene effettuato nel contesto delle attività di tale dipendente nell'UE (ossia il trattamento riguarda attività del titolare del trattamento al di fuori dell'UE), la mera presenza di un dipendente nell'UE non fa sì che il trattamento rientri nell'ambito di applicazione del RGPD. In altri termini, la mera presenza di un dipendente nell'UE non è di per sé sufficiente a innescare l'applicazione del RGPD, poiché il trattamento in questione, per rientrare nell'ambito di applicazione del RGPD, deve essere effettuato anche nel contesto delle attività del dipendente localizzato nell'UE.

Il fatto che il soggetto extra UE cui spetta la responsabilità del trattamento dei dati non disponga di una succursale o di una filiale in uno Stato membro non osta a che abbia uno stabilimento in tale Stato membro ai sensi del diritto dell'UE in materia di protezione dei dati.

Sebbene la nozione di stabilimento sia ampia, non è comunque senza limiti. Non è possibile concludere che il soggetto extra UE possiede uno stabilimento nell'Unione semplicemente perché il sito web dell'impresa è accessibile nell'Unione.[10]

Esempio 1

Una casa automobilistica con sede negli Stati Uniti possiede, a Bruxelles, una società controllata al 100 % che supervisiona tutte le sue operazioni in Europa, compresi il marketing e la pubblicità.

La filiale belga può essere considerata un'organizzazione stabile, che esercita attività reali ed effettive in funzione della natura dell'attività economica condotta dalla casa automobilistica. Tale filiale, quindi, potrebbe essere considerata uno stabilimento nell'Unione ai sensi del RGPD.

Una volta appurato che un titolare o un responsabile del trattamento è stabilito nell'UE, dovrebbe seguire un'analisi *in concreto* per determinare se il trattamento in questione sia effettuato nel contesto delle attività di tale stabilimento e, di conseguenza, se sia applicabile l'articolo 3, paragrafo 1. Se un titolare o un responsabile del trattamento stabilito al di fuori dell'Unione esercita «un'attività reale ed effettiva, anche minima, [...] tramite un'organizzazione stabile», indipendentemente dalla sua forma giuridica (ad esempio, filiale, succursale, ufficio ecc.) nel territorio di uno Stato membro, si può ritenere che tale titolare o responsabile del trattamento abbia uno stabilimento in detto Stato membro.[11] È pertanto importante valutare se il trattamento dei dati personali sia effettuato «nell'ambito delle attività di» un tale stabilimento, come evidenziato al considerando 22.

b) Trattamento dei dati personali effettuato «nell'ambito delle attività» di uno stabilimento

L'articolo 3, paragrafo 1, conferma che non è necessario che il trattamento in questione sia effettuato «dal» pertinente stabilimento dell'UE; il titolare o il re-

sponsabile del trattamento è soggetto agli obblighi derivanti dal RGPD ogniqualvolta il trattamento è effettuato «nel contesto delle attività» del pertinente stabilimento di tale titolare o responsabile nell'Unione. Il CEPD consiglia di stabilire se il trattamento sia effettuato nell'ambito di uno stabilimento del titolare o del responsabile del trattamento nell'Unione, ai fini dell'articolo 3, paragrafo 1, caso per caso e sulla base di un'analisi in concreto. Ogni scenario va valutato individualmente nel merito, tenendo conto delle specifiche circostanze.

Il CEPD ritiene che, ai fini dell'articolo 3, paragrafo 1, la nozione di «*trattamento [...] effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento*» sia da interpretare alla luce della giurisprudenza pertinente. Da un lato, al fine di realizzare l'obiettivo di assicurare una protezione efficace e completa, l'espressione «nell'ambito delle attività di uno stabilimento» non può essere interpretata in senso restrittivo.[12] Dall'altro, l'esistenza di uno stabilimento ai sensi del RGPD non dovrebbe essere interpretata in senso troppo lato, giungendo così a concludere che l'esistenza di qualsiasi presenza nell'UE – anche connessa nella misura più remota con le attività di trattamento dati di un soggetto extra UE – sia sufficiente a far ricadere tale trattamento nell'ambito di applicazione del diritto dell'UE in materia di protezione dei dati. Di fatto, alcune attività commerciali svolte da un soggetto extra UE all'interno di uno Stato membro possono essere così lontane dal trattamento dei dati personali effettuato da tale soggetto che l'esistenza dell'attività commerciale nell'UE non sarebbe sufficiente a far rientrare il trattamento effettuato dal soggetto extra UE nell'ambito del diritto dell'UE in materia di protezione dei dati.[13]

L'esame dei due fattori illustrati di seguito può contribuire a determinare se il trattamento sia effettuato da un titolare o da un responsabile del trattamento nell'ambito del suo stabilimento dell'Unione.

i) Rapporto tra un titolare o un responsabile del trattamento al di fuori dell'Unione e il suo stabilimento nell'Unione

Le attività di trattamento dei dati di un titolare o di un responsabile del trattamento stabiliti al di fuori dell'UE possono essere inscindibilmente connesse alle attività di uno stabilimento locale in uno Stato membro e possono quindi innescare l'applicabilità del diritto dell'UE anche se, in realtà, tale stabilimento locale non ha alcun ruolo nel trattamento dei dati in sé.[14] Se da un'analisi caso per caso di elementi concreti emerge l'esistenza di un nesso indissolubile tra il trattamento di dati personali effettuato da un titolare o da un responsabile del trattamento extra UE e le attività di uno stabilimento nell'UE, il diritto dell'UE si applica a tale trattamento svolto dal soggetto extra UE a prescindere dal fatto che lo stabilimento nell'UE svolga o meno un ruolo nel suddetto trattamento.[15]

ii) Realizzazione di ricavi nell'Unione

La realizzazione di ricavi nell'UE da parte di uno stabilimento locale, nella misura in cui tali attività possono essere considerate «inscindibilmente connesse» al trattamento di dati personali che avviene al di fuori dell'UE e a

singoli individui nell'UE, può essere indicativa del fatto che un titolare o un responsabile del trattamento extra UE effettui un trattamento «nell'ambito delle attività dello stabilimento nell'UE» e può essere sufficiente a innescare l'applicazione del diritto dell'UE a tale trattamento.[16]

Il CEPD raccomanda alle organizzazioni extra UE di condurre una valutazione delle proprie attività di trattamento, in primo luogo stabilendo se siano trattati dati personali e in secondo luogo individuando eventuali collegamenti tra l'attività per la quale i dati vengono trattati e le attività svolte da qualsiasi istanza dell'organizzazione nell'Unione. Qualora venga individuato tale collegamento, la sua natura sarà fondamentale per stabilire se il RGPD si applichi al trattamento in questione e la relativa valutazione dovrà essere svolta, tra l'altro, con riguardo ai due elementi di cui sopra.

Esempio 2

Un sito web di e-commerce è gestito da una società con sede in Cina. Le attività di trattamento dei dati personali della società sono svolte esclusivamente in Cina. La società cinese ha aperto un ufficio europeo a Berlino per guidare e dirigere la prospezione commerciale e le campagne di marketing rivolte ai mercati dell'UE.

In questo caso, si può ritenere che le attività dell'ufficio europeo di Berlino siano inscindibilmente connesse al trattamento di dati personali effettuato dal sito web cinese di commercio elettronico, nella misura in cui la prospezione commerciale e le campagne di marketing rivolte ai mercati dell'UE servono per rendere redditizio il servizio offerto tramite il sito web di commercio elettronico. Il trattamento dei dati personali da parte della società cinese in relazione alle vendite nell'UE è infatti inscindibilmente connesso alle attività dell'ufficio europeo di Berlino inerenti alla prospezione commerciale e alle campagne di marketing rivolte al mercato UE. Il trattamento dei dati personali da parte della società cinese in relazione alle vendite nell'UE può quindi essere considerato come effettuato nell'ambito delle attività dell'ufficio europeo in quanto stabilimento nell'Unione. Questa attività di trattamento della società cinese sarà quindi soggetta alle disposizioni del RGPD di cui all'articolo 3, paragrafo 1.

Esempio 3

Una catena di hotel e resort in Sudafrica offre pacchetti attraverso il suo sito web, disponibile in inglese, tedesco, francese e spagnolo. La società non dispone né di un ufficio né di rappresentanza o un'organizzazione stabile nell'UE.

In questo caso, in assenza di qualsiasi rappresentanza o organizzazione stabile della catena di hotel e resort nel territorio dell'Unione, sembrerebbe

che nessuna entità collegata al titolare del trattamento in Sudafrica possa essere considerata uno stabilimento nell'UE ai sensi del RGPD. Il trattamento in questione, quindi, non può essere soggetto alle disposizioni del RGPD di cui all'articolo 3, paragrafo 1.

Occorre tuttavia analizzare in concreto se il trattamento effettuato da questo titolare stabilito al di fuori dell'UE possa essere soggetto al RGPD a norma dell'articolo 3, paragrafo 2.

c) Applicazione del RGPD allo stabilimento di un titolare o di un responsabile del trattamento nell'UE, a prescindere dal fatto che il trattamento avvenga o meno nell'Unione

A norma dell'articolo 3, paragrafo 1, il trattamento di dati personali nell'ambito delle attività di uno stabilimento di un titolare o di un responsabile del trattamento nell'Unione comporta l'applicazione del RGPD e i relativi obblighi per il titolare o il responsabile del trattamento in questione.

Il testo del RGPD specifica che il regolamento si applica al trattamento nell'ambito delle attività di uno stabilimento nell'UE «*indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*». Sono la presenza, attraverso uno stabilimento, di un titolare o di un responsabile del trattamento nell'UE e il fatto che il trattamento avviene nell'ambito delle attività di tale stabilimento a innescare l'applicazione del RGPD alle rispettive attività di trattamento. Il luogo del trattamento non è quindi pertinente al fine di determinare se il trattamento, effettuato nell'ambito delle attività di uno stabilimento nell'Unione europea, rientri o meno nel campo di applicazione del RGPD.

Esempio 4

Una società francese ha sviluppato un'applicazione di car-sharing destinata esclusivamente a clienti di Marocco, Algeria e Tunisia. Il servizio è disponibile solo in questi tre paesi ma tutte le attività di trattamento di dati personali sono svolte dal titolare del trattamento dei dati in Francia.

Sebbene la raccolta di dati personali avvenga in paesi extra UE, il successivo trattamento di tali dati, in questo caso, viene effettuato nell'ambito delle attività di uno stabilimento di un titolare del trattamento nell'Unione. Pertanto, benché il trattamento si riferisca ai dati personali di interessati che non si trovano nell'Unione europea, le disposizioni del RGPD si applicheranno al trattamento effettuato dalla società francese a norma dell'articolo 3, paragrafo 1.

Esempio 5

Una società farmaceutica con sede a Stoccolma ha collocato tutte le attività di trattamento in relazione ai dati dei suoi studi clinici nella propria filiale con sede a Singapore.

In questo caso, sebbene le attività di trattamento avvengano a Singapore, il trattamento è effettuato nell'ambito delle attività della società farmaceutica di Stoccolma, vale a dire di un titolare del trattamento stabilito nell'Unione. Al trattamento si applicano pertanto le disposizioni del RGPD, come previsto dall'articolo 3, paragrafo 1.

Nel determinare l'ambito territoriale di applicazione del RGPD, l'ubicazione geografica è importante ai sensi dell'articolo 3, paragrafo 1, per quanto riguarda il luogo di stabilimento

- del titolare o del responsabile del trattamento (è stabilito all'interno o al di fuori dell'Unione?);
- di qualsiasi presenza commerciale di un titolare o responsabile del trattamento extra UE (ha uno stabilimento nell'Unione?)

Tuttavia, l'ubicazione geografica è irrilevante ai fini dell'articolo 3, paragrafo 1, per quanto riguarda il luogo in cui viene effettuato il trattamento o in cui si trovano gli interessati di cui trattasi.

Il testo dell'articolo 3, paragrafo 1, non limita l'applicazione del RGPD al trattamento di dati personali di persone fisiche che si trovano nell'Unione. Il CEPD ritiene pertanto che qualsiasi trattamento di dati personali nell'ambito delle attività di uno stabilimento di un titolare o di un responsabile del trattamento nell'Unione rientri nell'ambito di applicazione del RGPD, indipendentemente dall'ubicazione o dalla nazionalità dell'interessato i cui dati personali sono oggetto di trattamento. Questo approccio è corroborato dal considerando 14 del RGPD in cui si afferma che «*[è] opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali*».

d) Applicazione del criterio di stabilimento al titolare del trattamento o al responsabile del trattamento

Per quanto riguarda le attività di trattamento che rientrano nell'ambito di applicazione dell'articolo 3, paragrafo 1, il CEPD ritiene che tali disposizioni si applichino a titolari e ai responsabili del trattamento le cui attività di trattamento vengono effettuate nell'ambito delle attività del rispettivo stabilimento nell'UE. Pur riconoscendo che i requisiti per stabilire il rapporto tra un titolare del trattamento e un responsabile del trattamento[17] non variano a seconda dell'ubicazione geografica del rispettivo stabilimento, il CEPD ritiene che nell'individuare i diversi obblighi derivanti dall'applicabilità del RGPD, come disposto dall'articolo

3, paragrafo 1, il trattamento effettuato da ciascun soggetto debba essere considerato separatamente.

Il RGPD prevede obblighi o disposizioni diversi e specifici nei riguardi di titolari e responsabili del trattamento; di conseguenza, qualora un titolare o un responsabile del trattamento sia soggetto al RGPD a norma dell'articolo 3, paragrafo 1, i rispettivi obblighi si applicheranno separatamente. In questo contesto, il CEPD ritiene in particolare che un responsabile del trattamento nell'UE non debba essere considerato uno stabilimento del titolare del trattamento ai sensi dell'articolo 3, paragrafo 1, unicamente in virtù del suo status di responsabile operante per conto di tale titolare.

L'esistenza di un rapporto tra un titolare del trattamento e un suo responsabile non comporta necessariamente l'applicazione del RGPD a entrambi, qualora uno di tali soggetti non sia stabilito nell'Unione.

Un ente che tratta dati personali per conto e su incarico di un altro ente (la società cliente) funge da responsabile del trattamento per la società cliente (il titolare del trattamento). Se un responsabile del trattamento è stabilito nell'Unione, è tenuto a ottemperare agli obblighi imposti ai responsabili del trattamento dal RGPD (gli «obblighi dei responsabili del trattamento previsti dal RGPD»). Se il titolare del trattamento che dà incarico al responsabile del trattamento è anch'egli stabilito nell'Unione, è tenuto a rispettare gli obblighi imposti ai titolari del trattamento dal RGPD (gli «obblighi dei titolari del trattamento previsti dal RGPD»). L'attività di trattamento che, quando svolta da un titolare del trattamento, rientra nell'ambito di applicazione del RGPD in virtù dell'articolo 3, paragrafo 1, non esula dall'ambito di applicazione del regolamento semplicemente perché tale titolare incarica un responsabile del trattamento non stabilito nell'Unione di effettuare la suddetta attività per suo conto.

i) Trattamento eseguito da un titolare del trattamento stabilito nell'UE che dà incarico a un responsabile del trattamento non stabilito nell'Unione

Nel caso in cui un titolare soggetto al RGPD ricorra a un responsabile ubicato al di fuori dell'Unione per una determinata attività di trattamento, dovrà comunque assicurare, mediante contratto o altro atto giuridico, che detto responsabile esegua il trattamento dei dati conformemente al RGPD. L'articolo 28, paragrafo 3, prevede che il trattamento eseguito da un responsabile del trattamento debba essere disciplinato da un contratto o altro atto giuridico. Il titolare del trattamento deve pertanto fare in modo di stipulare con il responsabile un contratto che risponda a tutti i requisiti di cui all'articolo 28, paragrafo 3. Inoltre, al fine di assicurare il rispetto degli obblighi che gli incombono ai sensi dell'articolo 28, paragrafo 1 (utilizzare esclusivamente un responsabile del trattamento che offra garanzie sufficienti ad attuare le opportune misure, in modo tale che il trattamento risponda ai requisiti del regolamento e tuteli i diritti degli interessati), è probabile che il titolare del trattamento debba prendere in considerazione la possibilità di imporre, per contratto, gli obblighi previsti dal RGPD ai propri responsabili del trattamento. In altri termini, il titolare del trattamento dovrebbe

assicurare che, in virtù di un contratto o di altro atto giuridico a norma del diritto dell'Unione o di uno Stato membro, il responsabile del trattamento non soggetto al RGPD rispetti gli obblighi di cui all'articolo 28, paragrafo 3.

Il responsabile del trattamento con sede al di fuori dell'Unione sarà pertanto soggetto, indirettamente, ad alcuni obblighi impostigli dal titolare del trattamento soggetto al RGPD, in virtù degli accordi contrattuali di cui all'articolo 28. Possono essere inoltre applicabili le disposizioni del capo V del RGPD.

Esempio 6

Un istituto di ricerca finlandese svolge attività di ricerca sulla popolazione sami. L'istituto vara un progetto che riguarda esclusivamente la popolazione sami in Russia. Per questo progetto l'istituto utilizza un responsabile del trattamento con sede in Canada.

Il titolare del trattamento finlandese è tenuto a utilizzare esclusivamente responsabili del trattamento che offrano garanzie sufficienti ad attuare le opportune misure, in modo tale che il trattamento risponda ai requisiti del RGPD e garantisca la tutela dei diritti degli interessati. Inoltre, deve sottoscrivere un accordo sul trattamento dei dati con il responsabile del trattamento canadese, i cui obblighi sono stipulati in tale atto giuridico.

ii) Trattamento nell'ambito delle attività di uno stabilimento di un responsabile del trattamento nell'Unione

Mentre la giurisprudenza ci fornisce una chiara interpretazione degli effetti del trattamento svolto nell'ambito delle attività di uno stabilimento nell'UE del titolare del trattamento, l'effetto del trattamento svolto nell'ambito delle attività di uno stabilimento nell'UE di un responsabile del trattamento è meno chiaro.

Il CEPD sottolinea che è importante considerare separatamente lo stabilimento del titolare e quello del responsabile del trattamento per determinare se ciascuno dei due soggetti sia, di per sé, «stabilito nell'Unione».

Innanzitutto occorre determinare se lo stesso titolare del trattamento abbia uno stabilimento nell'Unione ed esegua il trattamento di dati nell'ambito delle attività di tale stabilimento. Qualora si concluda che il titolare non esegue il trattamento nell'ambito del proprio stabilimento nell'Unione, tale titolare non è soggetto agli obblighi dei titolari del trattamento previsti dal RGPD in virtù dell'articolo 3, paragrafo 1 (sebbene possa comunque essere soggetto all'articolo 3, paragrafo 2). A meno che siano in gioco altri fattori, lo stabilimento nell'UE del responsabile del trattamento non è considerato uno stabilimento in relazione al titolare del trattamento.

Occorre quindi determinare se il responsabile del trattamento esegua il trattamento nell'ambito del proprio stabilimento nell'Unione. In questo caso, il responsabile è soggetto agli obblighi previsti dal RGPD per i responsabili del tratta-

mento nell'articolo 3, paragrafo 1. Tuttavia, ciò non comporta che il titolare extra UE diventi soggetto agli obblighi previsti dal RGPD per i titolari del trattamento. In altri termini, un titolare del trattamento «extra UE» (come descritto sopra) non diviene soggetto al RGPD semplicemente perché decide di avvalersi di un responsabile del trattamento nell'Unione.

Attraverso l'incarico attribuito a un responsabile del trattamento nell'Unione, il titolare del trattamento non soggetto al RGPD non esegue il trattamento «nell'ambito delle attività del responsabile del trattamento nell'Unione». Il trattamento è eseguito nell'ambito delle attività proprie del titolare; il responsabile presta semplicemente un servizio di trattamento dati[18] che non è «inscindibilmente connesso» alle attività del titolare del trattamento. Come sopra affermato, nel caso di un responsabile del trattamento stabilito nell'Unione che tratti i dati per conto di un titolare al di fuori dell'Unione e non soggetto al RGPD a norma dell'articolo 3, paragrafo 2, il CEPD ritiene che le attività di trattamento del titolare non ricadano nell'ambito di applicazione territoriale del RGPD soltanto perché il trattamento viene eseguito per suo conto da un responsabile stabilito nell'Unione. Tuttavia, anche se il titolare del trattamento dei dati non è stabilito nell'Unione e non è soggetto alle disposizioni del RGPD di cui all'articolo 3, paragrafo 2, il responsabile del trattamento dei dati, poiché è stabilito nell'Unione, è soggetto alle pertinenti disposizioni del RGPD di cui all'articolo 3, paragrafo 1.

Esempio 7

Un'impresa messicana di vendite al dettaglio stipula con un responsabile del trattamento stabilito in Spagna un contratto per il trattamento di dati personali relativi ai propri clienti. La società messicana offre e rivolge i propri servizi esclusivamente al mercato messicano e il suo trattamento di dati riguarda esclusivamente interessati al di fuori dell'Unione.

In questo caso, la società messicana non si rivolge a persone nel territorio dell'Unione attraverso l'offerta di beni o la prestazione di servizi, né esegue il monitoraggio del comportamento degli interessati nel territorio dell'Unione. Il trattamento eseguito dal titolare del trattamento dei dati stabilito al di fuori dell'Unione, di conseguenza, non è soggetto al RGPD a norma dell'articolo 3, paragrafo 2.

Le disposizioni del RGPD non si applicano al titolare del trattamento in virtù dell'articolo 3, paragrafo 1, in quanto quest'ultimo non tratta i dati personali nell'ambito delle attività di un suo stabilimento nell'Unione. Il responsabile del trattamento dei dati è stabilito in Spagna e il suo trattamento rientra pertanto nell'ambito di applicazione del RGPD in virtù dell'articolo 3, paragrafo 1. Tale responsabile è tenuto a rispettare gli obblighi imposti dal regolamento ai responsabili del trattamento per qualsiasi trattamento eseguito nell'ambito delle proprie attività.

Quando è un responsabile stabilito nell'Unione a eseguire il trattamento per conto di un titolare che non ha stabilimenti nell'Unione ai fini dell'attività di trattamento e che non rientra nell'ambito territoriale del RGPD a norma dell'articolo 3, paragrafo 2, tale responsabile è soggetto alle disposizioni pertinenti del RGPD indicate di seguito che sono direttamente applicabili ai responsabili del trattamento dei dati.

- Gli obblighi imposti ai responsabili del trattamento a norma dell'articolo 28, paragrafi 2, 3, 4, 5 e 6, sull'obbligatorietà di stipulare un contratto sul trattamento dei dati, a eccezione di quelli relativi all'assistenza prestata al titolare del trattamento nel rispettare gli obblighi di quest'ultimo a norma del RGPD.
- Il responsabile del trattamento e chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento che abbia accesso a dati personali non può trattare tali dati se non viene incaricato dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o di uno Stato membro, come sancito dall'articolo 29 e dall'articolo 32, paragrafo 4.
- Ove applicabile, il responsabile del trattamento dei dati tiene un registro di tutte le categorie di trattamenti svolti per conto del titolare, come previsto dall'articolo 30, paragrafo 2.
- Ove applicabile, il responsabile del trattamento, su richiesta, coopera con l'autorità di controllo nell'esecuzione dei compiti di quest'ultima, come sancito dall'articolo 31.
- Il responsabile del trattamento mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, come disposto dall'articolo 32.
- Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza di una violazione dei dati personali, a norma dell'articolo 33.
- Ove applicabile, il responsabile del trattamento designa un responsabile della protezione dei dati, come previsto dagli articoli 37 e 38.
- Le disposizioni sui trasferimenti di dati personali a paesi terzi o a organizzazioni internazionali a norma del capo V.

Inoltre, poiché il trattamento in questione sarebbe eseguito nell'ambito delle attività di uno stabilimento del responsabile nell'Unione, il CEPD ricorda che il responsabile del trattamento deve garantire che il proprio trattamento sia conforme ad altri obblighi previsti dalla normativa UE o nazionale. L'articolo 28, paragrafo 3 specifica inoltre che «*il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati*».

In linea con le posizioni adottate in precedenza dal Gruppo di lavoro "Articolo 29", il CEPD ritiene che il territorio dell'Unione non possa essere utilizzato come un «paradiso dei dati», ad esempio quando una determinata tipologia di trattamento solleva questioni etiche inammissibili,[19] e che al di là dell'applicazione della normativa UE sulla protezione dei dati personali, taluni obblighi giuridici, in particolare le norme europee e nazionali in materia di ordine pubblico, vada-

no comunque rispettate da qualsiasi responsabile del trattamento nell'Unione, indipendentemente da dove sia situato il titolare del trattamento. Questa riflessione tiene conto anche del fatto che, in quanto applicazione della normativa UE, le disposizioni derivanti dal RGPD e le leggi nazionali correlate sono soggette alla Carta dei diritti fondamentali dell'Unione.[20] Tuttavia, ciò non impone ai titolari del trattamento situati al di fuori dell'Unione obblighi ulteriori rispetto a quei trattamenti che non ricadono nell'ambito di applicazione territoriale del RGDP.

2. APPLICAZIONE DEL CRITERIO DELL'INDIRIZZAMENTO (TARGETING) DEL TRATTAMENTO (ARTICOLO 3, PARAGRAFO 2)

L'assenza di uno stabilimento nell'Unione non significa necessariamente che le attività di trattamento da parte di un titolare o di un responsabile del trattamento stabilito in un paese terzo siano escluse dall'ambito di applicazione del RGPD, in quanto l'articolo 3, paragrafo 2, precisa le circostanze nelle quali si applica il RGPD a un titolare o a un responsabile del trattamento non stabilito nell'Unione, a seconda delle attività di trattamento.

In questo contesto, il CEPD conferma che, in assenza di uno stabilimento nell'Unione, un titolare o un responsabile del trattamento non possono beneficiare del meccanismo di sportello unico previsto nell'articolo 56 del RGPD. Il meccanismo di cooperazione e coerenza del RGPD, infatti, si applica esclusivamente ai titolari e ai responsabili del trattamento con uno o più stabilimenti all'interno dell'Unione europea.[21]

Sebbene le presenti Linee guida abbiano lo scopo di chiarire l'ambito di applicazione territoriale del RGPD, il CEPD desidera sottolineare che i titolari e i responsabili del trattamento devono altresì tenere conto di altri testi applicabili, ad esempio la normativa settoriale dell'UE o degli Stati membri e le leggi nazionali. Diverse disposizioni del RGPD consentono infatti agli Stati membri di introdurre ulteriori condizioni e di definire un quadro di protezione dei dati specifico a livello nazionale in determinati settori o in relazione a specifiche situazioni di trattamento. I titolari e i responsabili del trattamento devono quindi garantire di conoscere, e rispettare, tali condizioni e quadri aggiuntivi, che possono variare da uno Stato membro all'altro. Le variazioni nelle disposizioni sulla protezione dei dati applicabili in ciascuno Stato membro sono particolarmente importanti in relazione alle disposizioni dell'articolo 8 (in base al quale l'età alla quale i minori possono prestare un consenso valido in relazione al trattamento dei propri dati da parte di servizi della società dell'informazione può variare tra 13 e 16 anni), dell'articolo 9 (in relazione al trattamento di categorie particolari di dati personali), dell'articolo 23 (limitazioni) o in relazione alle disposizioni contenute nel capo IX del RGPD (libertà d'espressione e di informazione; accesso del pubblico ai documenti ufficiali; numero di identificazione nazionale; trattamento nell'ambito dei rapporti di lavoro; trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o a fini statistici; obblighi di segretezza; chiese e associazioni religiose).

Ai sensi dell'articolo 3, paragrafo 2, del RGPD «*"i]l presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione*».

L'applicazione del «criterio dell'indirizzamento (targeting) del trattamento» nei confronti di interessati che si trovano nell'Unione, come disposto nell'articolo 3, paragrafo 2, può configurarsi in rapporto ad attività di trattamento svolte da un titolare o da un responsabile del trattamento non stabiliti nell'Unione con riguardo a due diverse e alternative tipologie di attività, a condizione che tali attività di trattamento si riferiscano a interessati che si trovano nell'Unione. Oltre a essere applicabile solo al trattamento effettuato da un titolare o da un responsabile del trattamento non stabilito nell'Unione, il criterio dell'indirizzamento fa perno sostanzialmente su ciò che le "attività di trattamento" "riguardano", da valutare caso per caso.

Il CEPD sottolinea che un titolare o un responsabile del trattamento può essere soggetto al RGPD in relazione ad alcune delle rispettive attività di trattamento, ma non in relazione ad altre. L'elemento determinante per l'applicazione territoriale del RGPD ai sensi dell'articolo 3, paragrafo 2, risiede nella valutazione delle attività di trattamento in questione.

Nell'esaminare le condizioni per l'applicazione del criterio dell'indirizzamento (targeting) del trattamento, il CEPD raccomanda quindi un approccio bifasico, al fine di determinare in primo luogo e il trattamento si riferisca a dati personali di interessati che si trovano nell'Unione e, in secondo luogo, se riguardi l'offerta di beni o la prestazione di servizi o il monitoraggio del comportamento degli interessati nell'Unione.

a) Interessati nell'Unione

Il testo dell'articolo 3, paragrafo 2, fa riferimento a «*dati personali di interessati che si trovano nell'Unione*». L'applicazione del criterio dell'indirizzamento del trattamento, quindi, non è limitata dalla cittadinanza, dalla residenza o da altri elementi propri della condizione giuridica dell'interessato i cui dati personali sono oggetto di trattamento. Nel considerando 14, che conferma questa interpretazione, si legge che «*[è] opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali*».

Questa disposizione del RGPD riflette la normativa primaria dell'UE, che stabilisce del pari un ampio ambito di applicazione per la tutela dei dati personali, non limitato ai cittadini UE, attraverso l'articolo 8 della Carta dei diritti fondamentali, in base al quale il diritto alla tutela dei dati personali non è limitato, bensì garantito a «ogni individuo».[22]

Sebbene l'ubicazione dell'interessato nel territorio dell'Unione sia un fattore determinante per l'applicazione del criterio dell'indirizzamento del trattamento, come disposto dall'articolo 3, paragrafo 2, il CEPD ritiene che la nazionalità o la condizione giuridica di un interessato che si trova nell'Unione non possa limitare o restringere l'ambito di applicazione territoriale del regolamento.

Il requisito secondo cui l'interessato deve trovarsi nell'Unione va valutato nel momento in cui avviene la pertinente attività che ne innesca l'applicazione, vale a dire nel momento dell'offerta di beni o della prestazione di servizi o nel momento in cui viene monitorato il comportamento, indipendentemente dalla durata dell'offerta o del monitoraggio effettuato.

Il CEPD ritiene comunque che, in relazione alle attività di trattamento inerenti all'offerta di servizi, la disposizione sia rivolta alle attività che intenzionalmente, e non già inavvertitamente o fortuitamente, sono indirizzate a individui che si trovano nell'UE. Di conseguenza, se il trattamento riguarda un servizio offerto esclusivamente a individui al di fuori dell'UE e non viene sospeso quando questi ultimi entrano nell'UE, il trattamento correlato non è soggetto al RGPD. In questo caso, il trattamento non si riferisce all'indirizzamento intenzionale a persone che si trovano nell'UE, bensì all'indirizzamento a persone al di fuori dell'UE e tale indirizzamento proseguirà a prescindere dalla circostanza che dette persone restino al di fuori dell'UE o si rechino in visita nell'Unione.

Esempio 8

Un'impresa australiana offre un servizio mobile di notizie e contenuti video basati sulle preferenze e gli interessi degli utenti. Questi ultimi possono ricevere aggiornamenti quotidiani o settimanali. Il servizio è offerto esclusivamente a utenti ubicati in Australia, che devono fornire un numero di telefono australiano all'atto dell'abbonamento.

Un abbonato australiano del servizio si reca in Germania in vacanza e continua a utilizzare il servizio.

Sebbene l'abbonato australiano possa utilizzare il servizio durante il suo soggiorno nell'UE, il servizio non è «indirizzato» a persone che si trovano nell'Unione, bensì solo a persone in Australia; pertanto il trattamento dei dati personali da parte dell'impresa australiana non ricade nell'ambito di applicazione del RGPD.

Esempio 9

Una start-up stabilita negli Stati Uniti, senza alcuna presenza commerciale né stabilimento nell'UE, fornisce un'applicazione di mappe urbane per turisti. L'applicazione tratta i dati personali riguardanti l'ubicazione dei clienti che fanno uso dell'app (gli interessati) non appena questi ultimi

l'applicazione nella città che stanno visitando, al fine di offrire pubblicità mirata per luoghi da visitare, ristoranti, bar e alberghi. L'applicazione è disponibile per le visite turistiche di New York, San Francisco, Toronto, Parigi e Roma.

La start-up statunitense, mediante la sua applicazione di mappe urbane, si indirizza specificamente a persone fisiche che si trovano nell'Unione (nella fattispecie Parigi e Roma) offrendo loro i propri servizi quando queste si trovano nell'UE. Il trattamento dei dati personali degli interessati che si trovano nell'UE in relazione all'offerta del servizio ricade nell'ambito di applicazione del RGPD, come disposto dall'articolo 3, paragrafo 2, lettera a). Inoltre, trattando i dati di ubicazione dell'interessato al fine di offrire pubblicità mirata sulla base di tale ubicazione, le attività di trattamento riguardano anche il monitoraggio del comportamento di persone fisiche nell'Unione. Il trattamento della start-up statunitense, quindi, ricade nell'ambito di applicazione del RGPD anche ai sensi dell'articolo 3, paragrafo 2, lettera b).

Il CEPD desidera inoltre sottolineare che il fatto di trattare i dati personali di una persona fisica nell'Unione non è sufficiente, di per sé, a configurare l'applicabilità del RGPD alle attività di trattamento di un titolare o di un responsabile del trattamento non stabilito nell'Unione. Oltre a questo, infatti, tali attività devono sempre «indirizzarsi» a persone fisiche che si trovano nell'UE, in quanto vengono offerti loro beni o servizi o ne viene monitorato il comportamento (come chiarito ulteriormente in seguito).

Esempio 10

Un cittadino statunitense si reca in vacanza in Europa. Durante il suo soggiorno scarica e utilizza un'app di notizie offerta da un'impresa degli Stati Uniti. L'app è indirizzata esclusivamente al mercato statunitense, elemento che emerge dalle condizioni d'uso dell'applicazione e dall'indicazione del dollaro USA come unica valuta disponibile per il pagamento. La raccolta dei dati personali del turista statunitense effettuata da parte dell'impresa americana attraverso l'app non è soggetta al RGPD.

Inoltre, si deve rilevare che il trattamento dei dati personali di cittadini o residenti dell'UE effettuato in un paese terzo non comporta l'applicazione del RGPD fintantoché tale trattamento non riguarda una specifica offerta rivolta a persone fisiche nell'UE o il monitoraggio del loro comportamento nell'Unione.

Esempio 11

Alcuni clienti di una banca di Taiwan risiedono sull'isola ma hanno la cittadinanza tedesca. La banca opera solo a Taiwan e le sue attività non sono rivolte al mercato dell'UE. Il trattamento che la banca esegue sui dati personali dei suoi clienti tedeschi non è soggetto al RGPD.

Esempio 12

L'autorità competente in materia di immigrazione in Canada tratta i dati personali di cittadini dell'UE quando questi ultimi entrano nel territorio canadese, al fine di esaminare le loro richieste di visto. Questo trattamento non è soggetto al RGPD.

b) Offerta di beni o prestazione di servizi a interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato

La prima attività che innesca l'applicazione dell'articolo 3, paragrafo 2, è «l'offerta di beni o la prestazione di servizi», un concetto approfondito dalla normativa e dalla giurisprudenza UE, di cui va tenuto conto nell'applicazione del criterio dell'indirizzamento del trattamento. L'offerta di servizi comprende anche l'offerta di servizi della società dell'informazione, definita nell'articolo 1, paragrafo 1, punto b), della direttiva (UE) 2015/1535,[23] come «qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio pr*estato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi*».

L'articolo 3, paragrafo 2, lettera a), specifica che il criterio dell'indirizzamento del trattamento riguardante l'offerta di beni o la prestazione di servizi si applica indipendentemente dall'obbligatorietà di un pagamento dell'interessato. La possibilità di considerare l'attività di un titolare o di un responsabile del trattamento non stabilito nell'Unione come un'offerta di un bene o la prestazione di un servizio non dipende, quindi, dall'effettuazione di un pagamento in cambio dei beni forniti o dei servizi prestati.[24]

Esempio 13

Un'impresa statunitense, senza alcuno stabilimento nell'UE, tratta i dati personali dei suoi dipendenti in viaggio d'affari temporaneo in Francia, Belgio e nei Paesi Bassi per scopi relativi alle risorse umane, in particolare per procedere al rimborso delle spese di alloggio e al pagamento della loro indennità giornaliera, che varia a seconda del paese in cui si trovano.

In questa situazione, sebbene l'attività di trattamento sia collegata specifi-

camente a persone sul territorio dell'Unione (cioè i dipendenti che si trovano temporaneamente in Francia, Belgio e nei Paesi Bassi), essa non riguarda l'offerta di un servizio a tali persone, ma fa invece parte del trattamento necessario affinché il datore di lavoro ottemperi ai propri obblighi contrattuali e agli obblighi in materia di risorse umane relativamente all'impiego delle stesse. L'attività di trattamento non riguarda un'offerta di servizi e non è pertanto soggetta alla disposizione del RGPD di cui all'articolo 3, paragrafo 2, lettera a).

Un altro elemento chiave da tenere presente nel determinare se sia soddisfatto il criterio dell'indirizzamento del trattamento di cui all'articolo 3, paragrafo 2, lettera a), consiste nel verificare se l'offerta di beni o servizi sia rivolta a una persona nell'Unione o, in altre parole, se la condotta da parte del titolare del trattamento, che determina i mezzi e gli scopi del trattamento stesso, dimostra la sua intenzione di offrire beni o servizi a un interessato che si trova nell'Unione. Il considerando 23 del RGPD chiarisce infatti che «*[p]er determinare se tale titolare o responsabile del trattamento stia offrendo beni o servizi agli interessati che si trovano nell'Unione, è opportuno verificare se risulta che il titolare o il responsabile del trattamento intenda fornire servizi agli interessati in uno o più Stati membri dell'Unione*».

Lo stesso considerando specifica ulteriormente che «*[m]entre la semplice accessibilità del sito web del titolare del trattamento, del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione possono evidenziare l'intenzione del titolare o del responsabile del trattamento di offrire beni o servizi agli interessati nell'Unione*».

Gli elementi elencati nel considerando 23 rispecchiano e sono in linea con la giurisprudenza della CGUE riferita al regolamento n. 44/2001[25] concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, e in particolare il suo articolo 15, paragrafo 1, lettera c). Nella sentenza *Pammer/Reederei Karl Schlüter GmbH & Co e Hotel Alpenhof/Heller* (cause riunite C-585/08 e C-144/09), alla Corte era stato chiesto di chiarire che cosa significhi «attività diretta» ai sensi dell'articolo 15, paragrafo 1, lettera c), del regolamento n. 44/2001 (Bruxelles I). La CGUE ha ritenuto che, al fine di determinare se sia possibile considerare l'attività di un commerciante come «diretta» verso lo Stato membro in cui sono domiciliati i consumatori, ai sensi dell'articolo 15, paragrafo 1, lettera c), del regolamento Bruxelles I, il commerciante deve avere manifestato la propria intenzione di instaurare rapporti commerciali con tali consumatori. In questo contesto, la CGUE ha valutato le prove atte a dimostrare che era nell'intenzione del commerciante fare affari con consumatori domiciliati in uno Stato membro.

Sebbene la nozione di «dirigere un'attività» differisca dall'«offerta di beni o ser-

vizi», il CEPD ritiene che la giurisprudenza sopra ricordata nella causa *Pammer/Reederei Karl Schlüter GmbH & Co e Hotel Alpenhof/Heller* (cause riunite C-585/08 e C-144/09)[26] potrebbe risultare utile nel valutare se siano offerti beni o servizi a un interessato nell'Unione. Tenendo conto delle circostanze specifiche del caso, si potrebbero prendere in considerazione, inter alia, i fattori che seguono, anche congiuntamente:

- l'UE, o almeno uno Stato membro, sono indicati nominativamente in riferimento al bene o al servizio offerto;
- il titolare o il responsabile del trattamento paga il gestore di un motore di ricerca per un servizio di posizionamento su Internet al fine di facilitare l'accesso al proprio sito da parte dei consumatori dell'Unione; oppure il titolare o il responsabile del trattamento ha avviato campagne pubblicitarie e di marketing rivolte al pubblico di un paese dell'UE;
- la natura internazionale dell'attività in questione, come ad esempio certe attività turistiche;
- la menzione di indirizzi o numeri di telefono appositi da utilizzare da un paese dell'UE;
- l'uso di un nome di dominio di primo livello diverso da quello del paese terzo in cui il titolare o il responsabile del trattamento è stabilito, ad esempio «.de», oppure l'uso di nomi di dominio di primo livello neutri, ad esempio «.eu»;
- la descrizione delle istruzioni di viaggio da uno o più Stati membri dell'UE verso il luogo in cui viene fornito il servizio;
- la menzione di una clientela internazionale composta di clienti domiciliati in vari Stati membri dell'UE, in particolare mediante la presentazione di scritture contabili redatte da tali clienti;
- l'uso di una lingua o una valuta diverse da quelle generalmente utilizzate nel paese del commerciante, in particolare una lingua o una valuta di uno o più Stati membri dell'UE;
- il titolare del trattamento dei dati offre la consegna di beni negli Stati membri dell'UE.

Come già menzionato, diversi degli elementi elencati sopra, se presi singolarmente, possono non equivalere a una chiara indicazione dell'intenzione di un titolare del trattamento dei dati di offrire beni o servizi a interessati nell'Unione; tuttavia, ciascuno di essi dovrebbe essere preso in considerazione nello specifico della situazione concreta al fine di determinare se i fattori relativi alle attività commerciali del titolare dei dati possano, nel loro insieme, configurare un'offerta di beni o servizi rivolta a interessati nell'Unione.

È comunque importante ricordare che il considerando 23 conferma come la mera accessibilità del sito web del titolare del trattamento, del responsabile del trattamento o di un intermediario nell'Unione, la menzione sul sito web del suo indirizzo di posta elettronica o geografico o del suo numero di telefono senza un codice internazionale non costituiscono, di per sé, una prova sufficiente a dimostrare l'intenzione del titolare o del responsabile del trattamento di offrire beni o servizi a un interessato che si trova nell'Unione. In questo contesto, il CEPD

ricorda che quando i beni o i servizi sono forniti a una persona sul territorio dell'Unione in modo involontario o fortuito, il relativo trattamento dei dati personali non rientrerebbe nell'ambito di applicazione territoriale del RGPD.

Esempio 14

Un sito web, stabilito e gestito in Turchia, offre servizi per la creazione, l'editing, la stampa e la spedizione di album fotografici di famiglia personalizzati. Il sito è disponibile in inglese, francese, olandese e tedesco e i pagamenti possono essere effettuati in euro. Sulle sue pagine è indicato che gli album fotografici possono essere consegnati per posta esclusivamente in Francia, nei paesi del Benelux e in Germania.

In questo caso, è chiaro che la creazione, l'editing e la stampa di album fotografici di famiglia costituiscono un servizio ai sensi della normativa UE. Il fatto che il sito web sia disponibile in quattro lingue dell'Unione e che gli album fotografici possano essere consegnati per posta in sei Stati membri dell'UE dimostra l'intenzione del sito web turco di offrire i propri servizi a individui nell'Unione.

Di conseguenza, è chiaro che il trattamento effettuato dal sito web turco, in quanto titolare del trattamento dei dati, riguarda l'offerta di un servizio a interessati nell'Unione ed è quindi soggetto agli obblighi e alle disposizioni del RGPD, come sancito nel suo articolo 3, paragrafo 2, lettera a).

Conformemente all'articolo 27, il titolare del trattamento dei dati deve designare un rappresentante nell'Unione.

Esempio 15

Un'impresa privata con sede a Monaco tratta i dati personali dei suoi dipendenti ai fini del pagamento del loro stipendio. Un gran numero di dipendenti dell'impresa è costituito da residenti francesi e italiani.

In questo caso, sebbene il trattamento effettuato dall'impresa si riferisca a interessati in Francia e in Italia, esso non avviene nel contesto di un'offerta di beni o servizi. La gestione delle risorse umane, infatti, compreso il pagamento dello stipendio da parte di un'impresa di un paese terzo, non può essere considerata un'offerta di servizi ai sensi dell'articolo 3, paragrafo 2, lettera a). Il trattamento in questione non riguarda l'offerta di beni o servizi agli interessati nell'Unione (né il monitoraggio del loro comportamento) e, di conseguenza, non è soggetto alle disposizioni del RGPD, come sancito dall'articolo 3.

Questa valutazione fa salva la normativa applicabile del paese terzo interessato.

Esempio 16

Un'università svizzera di Zurigo avvia un processo di selezione per il suo master, mettendo a disposizione una piattaforma online nella quale i candidati possono caricare il proprio CV e la lettera di accompagnamento, unitamente ai propri recapiti. Il processo di selezione è aperto a qualsiasi studente con un adeguato livello di competenza linguistica in tedesco e in inglese e in possesso di una laurea. La pubblicità dell'università non è specificamente rivolta a studenti di università dell'UE e i pagamenti sono accettati esclusivamente in valuta svizzera.

Poiché non vi è alcuna distinzione o specifica per gli studenti provenienti dall'Unione nel processo di candidatura e selezione per questo master, non è possibile stabilire se l'università svizzera abbia l'intenzione di indirizzarsi agli studenti di un particolare Stato membro dell'UE. Il livello adeguato di competenza linguistica in tedesco e in inglese è un requisito generale che vale per qualsiasi candidato, sia esso un residente svizzero, una persona nell'Unione o uno studente di un paese terzo. In assenza di altri fattori che indichino che il master è indirizzato specificamente a studenti negli Stati membri dell'UE, non è possibile stabilire se il trattamento in questione riguardi l'offerta di un servizio di istruzione a interessati nell'Unione; pertanto tale trattamento non è soggetto alle disposizioni del RGPD.

L'università svizzera offre inoltre corsi estivi di relazioni internazionali e annuncia questa offerta specificamente nelle università tedesche e austriache per ottenere la massima adesione ai corsi. In questo caso è chiara l'intenzione dell'università svizzera di offrire tale servizio a interessati nell'Unione e quindi le attività di trattamento correlate sono soggette al RGPD.

c) Monitoraggio del comportamento degli interessati

Il secondo tipo di attività che comporta l'applicazione dell'articolo 3, paragrafo 2, è il monitoraggio del comportamento degli interessati nella misura in cui il loro comportamento avviene all'interno dell'Unione.

Il considerando 24 chiarisce che «*[è] opportuno che anche il trattamento dei dati personali degli interessati che si trovano nell'Unione ad opera di un titolare del trattamento o di un responsabile del trattamento non stabilito nell'Unione sia soggetto al presente regolamento quando è riferito al monitoraggio del comportamento di detti interessati, nella misura in cui tale comportamento ha luogo all'interno dell'Unione*».

Affinché l'articolo 3, paragrafo 2, lettera b), configuri l'applicazione del RGPD, il monitoraggio del comportamento deve innanzitutto riguardare un interessato nell'Unione e, come criterio cumulativo, deve avvenire all'interno del territorio dell'UE.

La natura dell'attività di trattamento che può essere considerata monitoraggio del comportamento è specificata ulteriormente nel considerando 24, nel quale si legge che *[p]er stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali]*. Benché il considerando 24 menzioni esclusivamente il monitoraggio di un comportamento attraverso il tracciamento di una persona su internet, il CEPD ritiene che, nel determinare se un'attività di trattamento equivalga al monitoraggio di un comportamento, si debba tenere conto anche del tracciamento attraverso altri tipi di rete o di tecnologie che comportano il trattamento di dati personali, ad esempio mediante dispositivi indossabili e altri dispositivi intelligenti.

Contrariamente alla disposizione dell'articolo 3, paragrafo 2, lettera a), né l'articolo 3, paragrafo 2, lettera b), né il considerando 24 prevedono l'«intenzione di indirizzarsi a» un soggetto da parte del titolare o del responsabile del trattamento quale elemento in qualche misura necessario al fine di determinare se l'attività di monitoraggio comporti l'applicazione del RGPD alle attività di trattamento. Ad ogni modo, l'uso della parola «monitoraggio» implica che il titolare del trattamento abbia in mente uno scopo specifico per la raccolta e il successivo riutilizzo dei dati pertinenti sul comportamento di una persona fisica all'interno dell'UE. Il CEPD non ritiene che qualsiasi raccolta o analisi online di dati personali di persone fisiche nell'UE debba essere considerata automaticamente un «monitoraggio».

Occorre valutare lo scopo perseguito dal titolare del trattamento mediante l'esecuzione di detto trattamento e, in particolare, qualsiasi successiva analisi comportamentale o tecnica di profilazione che riguardi i dati in questione. Il CEPD tiene conto del testo del considerando 24, secondo cui, per determinare se il trattamento comporti il monitoraggio del comportamento di un interessato, è fondamentale considerare il tracciamento di persone fisiche su Internet, compreso l'eventuale ricorso successivo a tecniche di profilazione.

L'applicazione dell'articolo 3, paragrafo 2, lettera b), nei casi in cui il titolare o il responsabile del trattamento effettui il monitoraggio del comportamento di interessati che si trovano nell'Unione, potrebbe quindi comprendere una vasta gamma di attività, fra cui in particolare:

- pubblicità comportamentale
- attività di geolocalizzazione, in particolare a scopi di marketing
- tracciamento online attraverso l'uso di cookies o altre tecniche apposite quali, ad esempio, il *fingerprinting* del browser
- servizi online di diete personalizzate e analisi mediche
- CCTV (televisione a circuito chiuso)
- indagini di mercato e altri studi comportamentali basati su profili individuali
- monitoraggio o comunicazione regolare sullo stato di salute di un individuo

Esempio 17

Un'impresa di consulenza stabilita negli Stati Uniti fornisce consulenza sull'allestimento di negozi al dettaglio a un centro commerciale in Francia, sulla base di un'analisi dei movimenti dei clienti attraverso il centro commerciale, raccolti mediante il tracciamento Wi-Fi.

L'analisi dei movimenti di un cliente all'interno del centro mediante il tracciamento Wi-Fi è equivalente al monitoraggio del comportamento del soggetto. In questo caso, il comportamento degli interessati ha luogo nell'Unione dal momento che il centro commerciale si trova in Francia. L'impresa di consulenza, in quanto titolare del trattamento dei dati, è quindi soggetta al RGPD per quanto riguarda il trattamento di tali dati ai fini di cui sopra, come disposto nel suo articolo 3, paragrafo 2, lettera b).

Conformemente all'articolo 27, il titolare del trattamento deve designare un rappresentante nell'Unione.

Esempio 18

Uno sviluppatore di app, stabilito in Canada e senza alcuno stabilimento nell'Unione, esegue il monitoraggio del comportamento di interessati nell'Unione ed è quindi soggetto al RGPD, come disposto dall'articolo 3, paragrafo 2, lettera b). Lo sviluppatore utilizza un responsabile del trattamento stabilito negli Stati Uniti per l'ottimizzazione dell'app e a scopi di manutenzione.

In relazione a questo trattamento, il titolare del trattamento canadese ha l'obbligo di servirsi esclusivamente di responsabili del trattamento idonei e di garantire che i suoi obblighi a norma del RGPD siano riportati nel contratto o nell'atto giuridico che disciplina il rapporto con il suo responsabile del trattamento negli Stati Uniti, come sancito nell'articolo 28.

d) Responsabile del trattamento non stabilito nell'Unione

I trattamenti «riguardanti» l'attività di indirizzamento dalla quale discende l'applicazione dell'articolo 3, paragrafo 2, rientrano nell'ambito di applicazione territoriale del RGPD. Il CEPD ritiene che occorra un collegamento tra l'attività di trattamento e l'offerta di beni o servizi, ma si deve prendere in considerazione sia il trattamento eseguito da un titolare sia quello eseguito da un responsabile del trattamento, essendo entrambi rilevanti.

Quando il responsabile del trattamento non è stabilito nell'Unione, al fine di determinare se il suo trattamento possa essere soggetto al RGPD, conformemente all'articolo 3, paragrafo 2, è necessario stabilire se le attività di trattamento re-

alizzate da tale responsabile riguardino le attività di indirizzamento svolte dal titolare del trattamento dei dati.

Il CEPD ritiene che, ove le attività di trattamento svolte da un titolare del trattamento riguardino l'offerta di beni o servizi o il monitoraggio del comportamento di persone fisiche nell'Unione («indirizzamento»), qualsiasi responsabile incaricato di svolgere tale attività di trattamento per conto del titolare ricada, in relazione a tale trattamento, nell'ambito di applicazione del RGPD in virtù dell'articolo 3, paragrafo 2.

Il fatto che un'attività di trattamento possa essere caratterizzata come «indirizzamento» dipende dagli scopi e dai mezzi di tale trattamento; la decisione di indirizzarsi a persone fisiche che si trovano nell'Unione può essere presa esclusivamente da chi riveste la funzione di titolare del trattamento. Tale interpretazione non esclude la possibilità che il responsabile del trattamento partecipi attivamente alle attività di trattamento legate alla realizzazione dei criteri di indirizzamento (vale a dire, il responsabile del trattamento offre beni o servizi o svolge azioni di monitoraggio per conto del titolare del trattamento e su suo incarico).

Il CEPD ritiene, quindi, che ci si debba concentrare sulla connessione tra le attività di trattamento svolte dal responsabile e l'attività di indirizzamento intrapresa dal titolare del trattamento in questione.

Esempio 19

Un'impresa brasiliana vende ingredienti alimentari e ricette locali, rendendo disponibile quest'offerta di beni a persone nell'Unione e pubblicizzando i prodotti e offrendo la consegna in Francia, Spagna e Portogallo. In questo contesto, l'impresa incarica un responsabile del trattamento, anch'esso stabilito in Brasile, di predisporre offerte speciali per i clienti in Francia, Spagna e Portogallo sulla base dei loro precedenti ordini e di eseguire il relativo trattamento dei dati.

Le attività di trattamento eseguite dal responsabile, su incarico del titolare del trattamento, riguardano l'offerta di beni a interessati nell'Unione. Inoltre, elaborando queste offerte personalizzate, il responsabile effettua un monitoraggio diretto su interessati nell'UE. Il trattamento eseguito da tale responsabile è quindi soggetto al RGPD, come disposto dall'articolo 3, paragrafo 2.

Esempio 20

Un'impresa statunitense ha messo a punto un'app sulla salute e sullo stile di vita che consente agli utenti di registrare con l'impresa stessa i propri indicatori personali (ore di sonno, peso, pressione sanguigna, battito cardiaco, ecc.). L'app fornisce poi agli utenti consigli quotidiani di alimentazione

e raccomandazioni su attività sportive. Il trattamento viene effettuato dal titolare statunitense. L'app è utilizzabile da persone fisiche nell'Unione. Ai fini della conservazione dei dati, l'impresa statunitense utilizza un responsabile del trattamento stabilito negli Stati Uniti (fornitore di servizi cloud). Nella misura in cui l'impresa nordamericana esegue il monitoraggio del comportamento di persone fisiche nell'UE, gestendo l'app sulla salute e sullo stile di vita tale impresa si indirizza a persone fisiche nell'UE e il suo trattamento dei dati personali di persone fisiche nell'UE rientra nell'ambito di applicazione del RGPD, ai sensi dell'articolo 3, paragrafo 2.

Nell'esecuzione del trattamento su incarico e per conto dell'impresa statunitense, il fornitore di servizi cloud/responsabile del trattamento svolge un'attività di trattamento «riguardante» l'indirizzamento verso persone fisiche nell'UE da parte del proprio titolare del trattamento. Quest'attività di trattamento svolta dal responsabile per conto del proprio titolare rientra nell'ambito dell'applicazione del RGPD, ai sensi dell'articolo 3, paragrafo 2.

Esempio 21

Un'impresa turca offre pacchetti viaggio culturali in Medio Oriente con guide turistiche in inglese, francese e spagnolo. I pacchetti viaggio, in particolare, sono pubblicizzati e offerti attraverso un sito web, disponibile nelle tre lingue, che consente la prenotazione e il pagamento in EUR e in GBP. A scopi di marketing e di prospezione commerciale l'impresa incarica un responsabile del trattamento, un call center stabilito in Tunisia, di contattare gli ex clienti in Irlanda, Francia, Belgio e Spagna per ottenere riscontri sui loro viaggi precedenti e informarli di nuove offerte e destinazioni.
Il titolare del trattamento svolge un'attività di «indirizzamento» offrendo i propri servizi a persone fisiche nell'UE e tale trattamento rientra nell'ambito di applicazione dell'articolo 3, paragrafo 2.

Anche le attività di trattamento del responsabile tunisino, che promuove i servizi del titolare del trattamento nei confronti di persone fisiche nell'UE, riguardano l'offerta di servizi del titolare e, di conseguenza, rientrano nell'ambito di applicazione dell'articolo 3, paragrafo 2. Inoltre, in questo caso specifico il responsabile del trattamento tunisino partecipa attivamente alle attività di trattamento legate ai criteri di indirizzamento del trattamento stesso offrendo servizi per conto e su incarico del titolare turco.

e) Interazioni con altre disposizioni del RGPD e altre normative

Il CEPD valuterà ulteriormente anche l'interazione tra l'applicazione dell'ambito territoriale del RGPD, ai sensi dell'articolo 3, e le disposizioni sui trasferimenti internazionali di dati, a norma del capo V. Orientamenti supplementari potranno essere formulati a questo riguardo, qualora fosse necessario.

I titolari o i responsabili del trattamento non stabiliti nell'UE sono tenuti a rispettare le leggi nazionali dei paesi terzi in relazione al trattamento dei dati personali. Tuttavia, qualora tale trattamento riguardi attività di indirizzamento verso persone fisiche nell'Unione, a norma dell'articolo 3, paragrafo 2, il titolare del trattamento deve rispettare il RGPD oltre che la normativa nazionale del proprio paese. Ciò vale a prescindere dal fatto che il trattamento sia eseguito conformemente a un obbligo giuridico vigente nel paese terzo o semplicemente per scelta del titolare del trattamento.

3. TRATTAMENTO DI DATI IN UN LUOGO SOGGETTO AL DIRITTO DI UNO STATO MEMBRO IN VIRTÙ DEL DIRITTO INTERNAZIONALE PUBBLICO

Ai sensi dell'articolo 3, paragrafo 3, «*[i]l presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico». Questa disposizione è meglio precisata attraverso il considerando 25, nel quale si legge che «[l]addove vige il diritto di uno Stato membro in virtù del diritto internazionale pubblico, ad esempio nella rappresentanza diplomatica o consolare di uno Stato membro, il presente regolamento dovrebbe applicarsi anche a un titolare del trattamento non stabilito nell'Unione*».

Il CEPD ritiene quindi che il RGPD si applichi al trattamento dei dati personali effettuato dalle ambasciate e dai consolati degli Stati membri situati al di fuori dell'UE, in quanto tale trattamento rientra nell'ambito di applicazione del RGPD in virtù dell'articolo 3, paragrafo 3. Una rappresentanza diplomatica o consolare di uno Stato membro, in qualità di titolare o responsabile del trattamento, sarebbe pertanto soggetta a tutte le pertinenti disposizioni del RGPD, anche per quanto riguarda i diritti dell'interessato, gli obblighi generali applicabili al titolare e al responsabile del trattamento e i trasferimenti di dati personali a paesi terzi o a organizzazioni internazionali.

Esempio 22

Il consolato olandese a Kingston, Giamaica, apre un procedimento di candidatura per l'assunzione di personale locale a sostegno della propria amministrazione.

Sebbene il consolato olandese a Kingston, Giamaica, non sia stabilito nell'Unione, il fatto che sia una rappresentanza consolare di un paese dell'UE nel quale vige il diritto dello Stato membro in virtù del diritto internazionale pubblico rende il RGPD applicabile al suo trattamento di dati personali, a norma dell'articolo 3, paragrafo 3.

Esempio 23

Una nave da crociera tedesca che viaggia in acque internazionali tratta i dati degli ospiti a bordo al fine di modulare l'offerta di intrattenimento in crociera.
Sebbene la nave si trovi al di fuori dell'Unione, in acque internazionali, il fatto che si tratti di una nave da crociera registrata in Germania significa che, in virtù del diritto internazionale pubblico, il RGPD è applicabile al suo trattamento di dati personali, a norma dell'articolo 3, paragrafo 3.

Pur non essendo legata all'applicazione dell'articolo 3, paragrafo 3, la situazione è diversa quando, in virtù del diritto internazionale, determinati organismi, organizzazioni o entità stabiliti nell'Unione usufruiscono di privilegi e immunità come, ad esempio, quelli sanciti nella Convenzione di Vienna sulle relazioni diplomatiche del 1961,[27] nella Convenzione di Vienna sulle relazioni consolari del 1963 o negli accordi sulla sede conclusi fra organizzazioni internazionali e i paesi che le ospitano nell'Unione. A questo riguardo, il CEPD ricorda che l'applicazione del RGPD fa salve le disposizioni del diritto internazionale, ad esempio quelle che disciplinano i privilegi e le immunità di missioni diplomatiche e rappresentanze consolari extra UE, nonché di organizzazioni internazionali. Al contempo, è importante ricordare che qualsiasi titolare o responsabile del trattamento che rientri nell'ambito di applicazione del RGPD per una determinata attività di trattamento e che scambi dati personali con tali organismi, organizzazioni ed entità, è tenuto a rispettare il RGPD comprese, ove applicabili, le norme sui trasferimenti a paesi terzi o a organizzazioni internazionali.

4. RAPPRESENTANTE DI TITOLARI O RESPONSABILI DEL TRATTAMENTO NON STABILITI NELL'UNIONE

I titolari o i responsabili del trattamento soggetti al RGPD a norma dell'articolo 3, paragrafo 2, sono tenuti a designare un rappresentante nell'Unione. Pertanto, un titolare o responsabile del trattamento non stabilito nell'Unione ma soggetto al RGPD che non designi un rappresentante nell'Unione agirebbe in violazione del regolamento.

Questa disposizione non è del tutto nuova; la direttiva 95/46/CE, infatti, prevedeva già un obbligo analogo. A norma della direttiva, questa disposizione riguardava i titolari del trattamento non stabiliti sul territorio comunitario che, a scopi di trattamento di dati personali, facevano uso di strumenti, automatizzati o meno, situati sul territorio di uno Stato membro. Il RGPD impone l'obbligo di designare un rappresentante nell'Unione a qualsiasi titolare o responsabile del trattamento che rientri nell'ambito di applicazione dell'articolo 3, paragrafo 2, a meno che siano soddisfatti i criteri di esenzione a norma dell'articolo 27, paragrafo 2. Al fine di facilitare l'applicazione di questa specifica disposizione, il CEPD ritiene necessario fornire ulteriori indicazioni sulla procedura di designazione, sugli obblighi di stabilimento e sulle responsabilità del rappresentante nell'Unione, come disposto nell'articolo 27.

È opportuno notare che un titolare o un responsabile del trattamento non stabilito nell'Unione che ha designato per iscritto un rappresentante nell'Unione, conformemente all'articolo 27 del RGPD, non ricade nell'ambito di applicazione dell'articolo 3, paragrafo 1; in altri termini, la presenza del rappresentante all'interno dell'Unione non configura uno «stabilimento» di tale titolare o responsabile del trattamento ai sensi dell'articolo 3, paragrafo 1.

a) Designazione di un rappresentante

Il considerando 80 chiarisce che «*[i]l rappresentante dovrebbe essere esplicitamente designato mediante mandato scritto del titolare del trattamento o del responsabile del trattamento ad agire per conto di questi ultimi con riguardo agli obblighi che a questi derivano dal presente regolamento. La designazione di tale rappresentante non incide sulla responsabilità generale del titolare del trattamento o del responsabile del trattamento ai sensi del presente regolamento. Tale rappresentante dovrebbe svolgere i suoi compiti nel rispetto del mandato conferitogli dal titolare del trattamento o dal responsabile del trattamento, anche per quanto riguarda la cooperazione con le autorità di controllo competenti per qualsiasi misura adottata al fine di garantire il rispetto del presente regolamento*».

Il mandato scritto cui fa riferimento il considerando 80 disciplina quindi i rapporti e gli obblighi tra il rappresentante nell'Unione e il titolare o il responsabile del trattamento dati stabilito al di fuori dell'UE, pur non incidendo sulla responsabilità generale di tale titolare o responsabile. Il rappresentante nell'Unione può essere una persona fisica o giuridica stabilita nell'UE e in grado di rappresentare un titolare o un responsabile del trattamento stabilito al di fuori dell'Unione in relazione ai loro rispettivi obblighi ai sensi del RGPD.

In concreto, la funzione di rappresentante nell'Unione può essere esercitata sulla base di un contratto di servizio concluso con una persona fisica o un'organizzazione e può quindi essere assunta da una vasta gamma di soggetti commerciali e non commerciali quali, ad esempio, studi legali, società di consulenza, imprese private ecc., a condizione che tali soggetti siano stabiliti nell'Unione. Un rappresentante può anche agire per conto di più titolari o responsabili del trattamento extra UE.

Quando la funzione di rappresentante è assunta da un'impresa o da qualsiasi altro tipo di organizzazione, si consiglia di designare un'unica persona come contatto principale e «responsabile» per conto di ogni titolare o responsabile del trattamento rappresentato. In generale, sarebbe anche utile specificare questi punti nel contratto di servizio.

In conformità del RGPD, il CEPD conferma che, quando più attività di trattamento di un titolare o di un responsabile rientrano nell'ambito di applicazione dell'articolo 3, paragrafo 2, del RGPD (e non è valida nessuna delle eccezioni dell'articolo 27, paragrafo 2, del RGPD), tale titolare o responsabile non è tenuto a designare più rappresentanti per ogni distinta attività di trattamento che rientra nell'ambito di applicazione dell'articolo 3, paragrafo 2. Il CEPD non ritiene che la funzione di rappresentante nell'Unione sia compatibile con il ruolo di respon-

sabile della protezione dei dati (RPD) esterno stabilito nell'Unione. L'articolo 38, paragrafo 3, fissa alcune garanzie fondamentali per contribuire ad assicurare che i responsabili della protezione dei dati possano svolgere i loro compiti con sufficiente autonomia all'interno della rispettiva organizzazione. In particolare, i titolari o i responsabili del trattamento devono assicurarsi che il responsabile della protezione dei dati «*non riceva alcuna istruzione per quanto riguarda l'esecuzione [dei suoi] compiti*». Il considerando 97 aggiunge che i RPD, «*dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente*».[28] Il requisito di un adeguato livello di autonomia e indipendenza del responsabile della protezione dei dati non sembra compatibile con la funzione di rappresentante nell'Unione. Il rappresentante è infatti soggetto a un mandato affidatogli da un titolare o da un responsabile del trattamento e agirà per suo conto e, quindi, dietro sue dirette istruzioni.[29] Il rappresentante riceve il mandato dal titolare o dal responsabile del trattamento che rappresenta, agendo per suo conto nell'esercizio dei propri compiti, e tale ruolo non può essere compatibile con lo svolgimento indipendente dei compiti e delle mansioni del responsabile della protezione dei dati.

Inoltre, a ulteriore integrazione di quanto sopra esposto, il CEPD ricorda la posizione già adottata dal Gruppo di lavoro "Articolo 29" secondo cui «*può insorgere un conflitto di interessi se, per esempio, a un RPD esterno si chiede di rappresentare il titolare o il responsabile in un giudizio che tocchi problematiche di protezione dei dati*».[30]

Analogamente, dato il possibile conflitto tra obblighi e interessi in caso di applicazione di misure, il CEPD non ritiene che la funzione di rappresentante di un titolare del trattamento nell'Unione sia compatibile con il ruolo di responsabile del trattamento per tale stesso titolare, soprattutto per quanto riguarda l'adempimento delle rispettive responsabilità.

Sebbene il RGPD non preveda, per il titolare del trattamento o il rappresentante stesso, alcun obbligo di notificare la designazione di quest'ultimo a un'autorità di controllo, il CEPD ricorda che, conformemente agli articoli 13, paragrafo 1, lettera a), e 14, paragrafo 1, lettera a), nell'ambito dei propri obblighi di informazione i titolari del trattamento forniscono agli interessati informazioni inerenti al proprio rappresentante nell'Unione. Tali informazioni devono essere incluse, ad esempio, [nell'informativa sulla privacy e] nelle comunicazioni fornite agli interessati previamente alla raccolta dei dati. Un titolare del trattamento non stabilito nell'Unione ma soggetto all'applicazione dell'articolo 3, paragrafo 2, che non informi gli interessati nell'Unione dell'identità del proprio rappresentante violerebbe i propri obblighi di trasparenza a norma del RGPD. Tali informazioni devono, inoltre, essere facilmente accessibili alle autorità di controllo al fine di facilitare loro la presa di contatto per esigenze di cooperazione.

Esempio 24

Il sito web di cui all'esempio 12, stabilito e gestito in Turchia, offre servizi per la creazione, l'editing, la stampa e la spedizione di album fotografici

di famiglia personalizzati. Il sito è disponibile in inglese, francese, olandese e tedesco e i pagamenti possono essere effettuati in euro o sterline. Sulle sue pagine è indicato che gli album fotografici possono essere consegnati per posta esclusivamente in Francia, nei paesi del Benelux e in Germania. Poiché questo sito web è soggetto al RGPD a norma dell'articolo 3, paragrafo 2, lettera a), il titolare del trattamento deve designare un rappresentante nell'Unione.

Il rappresentante deve essere stabilito in uno degli Stati membri in cui è disponibile il servizio offerto; nel caso in oggetto in Francia, Belgio, nei Paesi Bassi, in Lussemburgo e in Germania. Il nome e i recapiti del titolare del trattamento e del suo rappresentante nell'Unione devono essere inclusi nelle informazioni rese disponibili online per gli interessati, nel momento in cui questi ultimi iniziano a utilizzare il servizio creando il proprio album fotografico. Esse devono inoltre figurare nell'informativa generale sulla privacy del sito web.

b) Esenzioni dall'obbligo della designazione[31]

Sebbene l'applicazione dell'articolo 3, paragrafo 2, comporti l'obbligo di designare un rappresentante nell'Unione per i titolari o i responsabili del trattamento stabiliti al di fuori dell'Unione, l'articolo 27, paragrafo 2, prevede una deroga a tale designazione obbligatoria in due casi distinti:

- quando il trattamento è «occasionale, non include il trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10», e quando «è improbabile che [tale trattamento] presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento».

Conformemente alle posizioni adottate in precedenza dal Gruppo di lavoro "Articolo 29", il CEPD ritiene che un'attività di trattamento possa essere considerata «occasionale» esclusivamente se non viene effettuata regolarmente e si verifica al di fuori della normale attività commerciale del titolare o del responsabile del trattamento.[32]

[33]Inoltre, sebbene il RGPD non contenga una definizione di trattamento su larga scala, il Gruppo di lavoro "Articolo 29" ha raccomandato, nelle linee guida WP243 sui responsabili della protezione dei dati (RPD), di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala: il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; la durata, ovvero la persistenza, dell'attività di trattamento; la portata geografica dell'attività di trattamento.

Infine, il CEPD sottolinea che l'esenzione dall'obbligo della designazione, come disposto dall'articolo 27, fa riferimento al caso in cui sia «improbabile che [il trat-

tamento] presenti un rischio per i diritti e le libertà delle persone fisiche»[34]; pertanto, tale esenzione non è limitata ai soli trattamenti per i quali sia improbabile un rischio elevato per i diritti e le libertà degli interessati. Alla luce del considerando 75, nel valutare il rischio per i diritti e le libertà degli interessati occorre considerare sia la probabilità sia la gravità di tale rischio.

Il secondo caso in cui si applica la deroga suddetta riguarda:

- il trattamento effettuato «da un'autorità pubblica o da un organismo pubblico».

La qualifica di «autorità pubblica o organismo pubblico» riferita a un soggetto stabilito al di fuori dell'Unione dovrà essere valutata dall'autorità di controllo *in concreto* e caso per caso.[35] Il CEPD rileva che, attesa la natura dei compiti e delle missioni affidate, i casi in cui un'autorità pubblica o un organismo pubblico in un paese terzo offre beni o servizi a interessati nell'Unione, o ne monitora il comportamento che avviene all'interno dell'Unione, sono verosimilmente limitati.

c) Stabilimento in uno degli Stati membri nel quale si trovano gli interessati i cui dati personali sono oggetto di trattamento

Ai sensi dell'articolo 27, paragrafo 3, «il rappresentante è stabilito in uno degli Stati membri in cui si trovano gli interessati e i cui dati personali sono trattati nell'ambito dell'offerta di beni o servizi o il cui comportamento è monitorato». Nei casi in cui una cospicua parte degli interessati i cui dati personali vengono trattati si trovi in un determinato Stato membro, la raccomandazione del CEPD è, in termini di buona prassi, che il rappresentante sia stabilito in tale Stato membro. Tuttavia, il rappresentante deve continuare a essere facilmente accessibile per gli interessati che si trovano negli Stati membri nei quali non è stabilito e dove vengono offerti i beni o servizi oppure dove viene monitorato il comportamento.

Il CEPD conferma che il criterio per lo stabilimento del rappresentante nell'Unione è il luogo in cui si trovano gli interessati i cui dati personali sono oggetto di trattamento. Il luogo in cui si svolge il trattamento, anche se effettuato da un responsabile del trattamento stabilito in un altro Stato membro, in questo caso non è un fattore rilevante al fine di definire dove debba essere stabilito il rappresentante.

Esempio 25

Un'impresa farmaceutica indiana, senza presenza commerciale né stabilimento nell'Unione e soggetta al RGPD a norma dell'articolo 3, paragrafo 2, sponsorizza studi clinici effettuati da ricercatori (ospedali) in Belgio, Lussemburgo e nei Paesi Bassi. La maggior parte dei pazienti che partecipano agli studi clinici si trova in Belgio.

L'impresa farmaceutica indiana, in quanto titolare del trattamento, designa un rappresentante nell'Unione, stabilito in uno dei tre Stati membri

in cui i pazienti, in quanto interessati, partecipano allo studio clinico (Belgio, Lussemburgo e Paesi Bassi). Dal momento che la maggior parte dei pazienti è residente in Belgio, è consigliabile che anche il rappresentante sia stabilito nello stesso paese. In tal caso, il rappresentante in Belgio deve comunque essere facilmente accessibile agli interessati e alle autorità di controllo nei Paesi Bassi e in Lussemburgo.

In questo caso specifico, il rappresentante nell'Unione potrebbe essere il rappresentante legale dello sponsor nell'Unione, come previsto dall'articolo 74 del regolamento (UE) 536/2014 sugli studi clinici, a condizione che non funga da responsabile del trattamento per conto dello sponsor degli studi clinici, che sia stabilito in uno dei tre Stati membri, e che entrambe le funzioni siano disciplinate ed esercitate conformemente al rispettivo regime giuridico.

d) Obblighi e responsabilità del rappresentante

Il rappresentante nell'Unione agisce per conto del titolare o del responsabile del trattamento che rappresenta per quanto riguarda gli obblighi rispettivamente incombenti a norma del RGPD. Ciò comporta, in particolare, gli obblighi inerenti all'esercizio dei diritti degli interessati; di conseguenza, come già affermato a tale proposito, l'identità e i recapiti del rappresentante devono essere comunicati agli interessati conformemente agli articoli 13 e 14. Sebbene non sia di per sé responsabile del rispetto dei diritti degli interessati, il rappresentante deve facilitare la comunicazione tra gli interessati e il titolare o il responsabile del trattamento rappresentato, al fine di rendere effettivo l'esercizio dei diritti degli interessati stessi.

A norma dell'articolo 30, il rappresentante del titolare o del responsabile del trattamento tiene, in particolare, un registro delle attività di trattamento sotto la responsabilità di questi ultimi. Il CEPD ritiene che, sebbene la tenuta di tale registro sia un obbligo imposto sia al titolare o al responsabile del trattamento sia al rappresentante, il titolare o il responsabile del trattamento non stabilito nell'Unione è responsabile del contenuto principale e dell'aggiornamento del registro e deve, al contempo, fornire al proprio rappresentante tutte le informazioni, precise e aggiornate, in modo che anche quest'ultimo possa tenere e rendere disponibile il registro in qualsiasi momento. Al tempo stesso, è responsabilità propria del rappresentante essere in grado di fornire tali informazioni, in conformità dell'articolo 27, ad esempio quando funge da interlocutore di un'autorità di controllo a norma dell'articolo 27, paragrafo 4.

Come chiarito dal considerando 80, il rappresentante deve svolgere i propri compiti nel rispetto del mandato conferitogli dal titolare o dal responsabile del trattamento, anche per quanto riguarda la cooperazione con le autorità di controllo competenti in rapporto a qualsiasi misura adottata al fine di garantire il rispetto del regolamento. In concreto, ciò significa che un'autorità di controllo può rivolgersi al rappresentante in relazione a ogni questione inerente agli ob-

blighi di conformità di un titolare o di un responsabile del trattamento stabilito al di fuori dell'Unione e il rappresentante deve essere in grado di facilitare qualsiasi scambio di informazioni o passo procedurale che coinvolga un'autorità di controllo richiedente e un titolare o responsabile del trattamento stabilito al di fuori dell'Unione.

Con l'aiuto di un'équipe, se necessario, il rappresentante nell'Unione deve quindi essere in condizione di comunicare efficacemente con gli interessati e di cooperare con le autorità di controllo interessate. Ciò significa che tale comunicazione deve avvenire, in linea di massima, nella lingua o nelle lingue utilizzate dalle autorità di controllo e dagli interessati in questione; in alternativa, qualora ciò comporti difficoltà sproporzionate, il rappresentante deve utilizzare altri mezzi e tecniche al fine di garantire una comunicazione efficace. La presenza di un rappresentante è quindi essenziale per garantire che gli interessati e le autorità di controllo possano contattare facilmente il titolare o il responsabile del trattamento extra UE. In linea con il considerando 80 e l'articolo 27, paragrafo 5, la designazione di un rappresentante nell'Unione non influisce sulla responsabilità del titolare o del responsabile del trattamento a norma del RGPD e fa salve le controversie che potrebbero essere avviate nei confronti degli stessi. Il RGPD non stabilisce una responsabilità vicaria del rappresentante rispetto al titolare o al responsabile del trattamento che egli rappresenta nell'Unione.

Va tuttavia rilevato che la figura del rappresentante è stata introdotta proprio allo scopo di facilitare il collegamento con i titolari o i responsabili del trattamento e di garantire l'applicazione efficace del RGPD nei confronti dei titolari o dei responsabili del trattamento soggetti all''articolo 3, paragrafo 2, dello stesso. A tal fine, si è voluto consentire alle autorità di controllo di avviare procedimenti attuativi di misure nei confronti di titolari o responsabili del trattamento non stabiliti nell'Unione attraverso il loro rappresentante designato. Ciò comprende la possibilità, per le autorità di controllo, di indirizzare al rappresentante le misure correttive o le sanzioni amministrative pecuniarie e le altre sanzioni imposte al titolare o al responsabile del trattamento non stabilito nell'Unione, conformemente all'articolo 58, paragrafo 2, e all'articolo 83 del RGPD. La possibilità di ritenere un rappresentante direttamente responsabile è comunque limitata agli obblighi specificamente incombenti su tale rappresentante, di cui agli articoli 30 e 58, paragrafo 1, del RGPD.

Il CEPD, inoltre, sottolinea che l'articolo 50 del RGPD, in particolare, mira a facilitare l'applicazione della normativa in relazione ai paesi terzi e alle organizzazioni internazionali e che è in corso di valutazione lo sviluppo di ulteriori meccanismi di cooperazione internazionale a questo riguardo.

NOTE

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[2] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[3] Gruppo di lavoro "Articolo 29", WP169, Parere 1/2010 sui concetti di «responsabile [leggi: titolare] del trattamento» e «incaricato [leggi: responsabile] del trattamento», adottato il 16 febbraio 2010 e in corso di revisione da parte del CEPD.

[4] La definizione di «stabilimento principale» è pertinente soprattutto ai fini della determinazione della competenza delle autorità di controllo interessate secondo l'articolo 56 del RGPD. Si vedano le Linee guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento del Gruppo di lavoro "Articolo 29" (16/EN WP 244 rev.01), approvate dal CEPD.

[5] Considerando 22 del RGPD: «*Qualsiasi trattamento di dati personali effettuato nell'ambito delle attività di uno stabilimento di un titolare del trattamento o responsabile del trattamento nel territorio dell'Unione dovrebbe essere conforme al presente regolamento, indipendentemente dal fatto che il trattamento avvenga all'interno dell'Unione. Lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica*».

[6] Cfr. in particolare *Google Spain SL, Google Inc./AEPD, Mario Costeja González (C-131/12), Weltimmo/NAIH (C-230/14), Verein für Konsumenteninformation/Amazon EU (C-191/15) e Wirtschaftsakademie Schleswig-Holstein (C-210/16).*

[7] Weltimmo, punto 31.

[8] Weltimmo, punto 29.

[9] Weltimmo, punto 31.

[10] CGUE, Verein für Konsumenteninformation/Amazon EU Sarl, causa C-191/15, 28 luglio 2016, punto 76 (di seguito «Verein für Konsumenteninformation»).

[11] Si veda, in particolare, il punto 29 della sentenza Weltimmo, che evidenzia una concezione flessibile della nozione di stabilimento e chiarisce che «occorre valutare sia il grado di stabilità dell'organizzazione sia l'esercizio effettivo delle attività in tale altro Stato membro, prendendo in considerazione la natura specifica delle attività economiche e delle prestazioni di servizi in questione».

[12] Weltimmo, punto 25, e Google Spain, punto 53.

[13] Gruppo di lavoro "Articolo 29", WP 179, Aggiornamento del parere 8/2010 sul diritto applicabile alla luce della sentenza della CGUE nella causa Google Spain, 16 dicembre 2015

[14] CGUE, Google Spain, causa C-131/12

[15] Gruppo di lavoro "Articolo 29", WP 179, Aggiornamento del parere 8/2010 sulla legge applicabile alla luce della sentenza della CGUE nella causa Google Spain, 16 dicembre 2015

[16] Lo stesso può valere, ad esempio, per qualsiasi operatore straniero con un ufficio vendite o un altro tipo di presenza nell'UE, sebbene tale ufficio non svolga alcun ruolo nell'effettivo trattamento dei dati, in particolare nel caso in cui il trattamento sia effettuato nell'ambito dell'attività di vendita nell'UE e le attività dello stabilimento siano rivolte agli abitanti degli Stati membri in cui quest'ultimo ha sede (WP179 aggiornamento).

[17] Conformemente all'articolo 28, il CEPD fa presente che le attività di trattamento svolte da un responsabile per conto di un titolare del trattamento devono essere disciplinate da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri che vincoli il responsabile al titolare, e che i titolari devono utilizzare esclusivamente responsabili che offrono garanzie sufficienti ad attuare le opportune misure, in modo tale che il trattamento risponda ai requisiti del RGPD e garantisca la tutela dei diritti degli interessati.

[18] In questo contesto, anche l'offerta di un servizio di trattamento dati non può essere considerata l'offerta di un servizio a interessati nell'Unione.

[19] Gruppo di lavoro "Articolo 29", WP169, Parere 1/2010 sui

concetti di «responsabile [leggasi: titolare] del trattamento» e «incaricato [leggasi: responsabile] del trattamento», adottato il 16 febbraio 2010 e in corso di revisione da parte del CEPD.

[20] Carta dei diritti fondamentali dell'Unione europea (2012/C 326/02).

[21] Gruppo di lavoro "Articolo 29", WP244 rev.1, 13 dicembre 2016, Linee guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento, approvate dal CEPD.

[22] Carta dei diritti fondamentali dell'Unione europea, articolo 8, paragrafo 1, «[o]gni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano».

[23] Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione.

[24] Cfr., in particolare, CGUE, C-352/85, Bond van Adverteerders e altri/Stato olandese, 26 aprile 1988, punto 16), e CGUE, C-109/92, Wirth [1993] Racc. I-6447, punto 15.

[25] Regolamento (CE) n. 44/2001 del Consiglio, del 22 dicembre 2000, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale.

[26] È ancora più importante il fatto che, a norma dell'articolo 6 del regolamento (CE) n. 593/2008, del Parlamento europeo e del Consiglio, del 17 giugno 2008, sulla legge applicabile alle obbligazioni contrattuali (Roma I), in assenza di una scelta della legge applicabile, il criterio di «dirigere un'attività» verso il paese di residenza abituale del consumatore venga preso in considerazione per individuare la legge del luogo di residenza abituale del consumatore come la legge applicabile al contratto.

[27] http://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf

[28] WP29 Linee guida sui responsabili della protezione dei dati, WP 243 rev.01, approvate dal CEPD.

[29] Un responsabile esterno della protezione dei dati che funge anche da rappresentante nell'Unione non potrebbe, ad esempio, trovarsi in una situazione in cui gli viene affidato il compito, in qualità di rappresentante, di comunicare a un interessato una decisione o una misura adottata dal titolare o dal responsabile del trattamento che lui, in quanto responsabile della protezione dei dati, aveva ritenuto non conforme alle disposizioni del RGPD e che aveva sconsigliato.

[30] WP29 Linee guida sui responsabili della protezione dei dati, WP 243 rev.01, approvate dal CEPD.

[31] Parte dei criteri e dell'interpretazione formulata nel documento del Gruppo di lavoro "Articolo 29" WP243 rev.1 (Responsabile della protezione dei dati), approvato dal CEPD, possono essere utilizzati come fondamento per le esenzioni dall'obbligo di designazione.

[32] Documento di posizione del Gruppo di lavoro "Articolo 29" sulle deroghe all'obbligo di tenere registri delle attività di trattamento a norma dell'articolo 30, paragrafo 5, del RGPD.

[33] Gruppo di lavoro "Articolo 29", Linee guida sui responsabili della protezione dei dati (RPD), adottate il 13 dicembre 2016, versione emendata e adottata il 5 aprile 2017, WP 243 rev.01, approvate dal CEPD.

[34] Articolo 27, paragrafo 2, lettera a), del RGPD.

[35] Il RGPD non contiene una definizione di «un'autorità pubblica o un organismo pubblico». Il CEPD ritiene che tale concetto debba essere interpretato ai sensi della normativa nazionale. Di conseguenza, le autorità e gli organismi pubblici includono autorità nazionali, regionali e locali ma il concetto, ai sensi della normativa nazionale applicabile, generalmente comprende anche una serie di altri organismi disciplinati dal diritto pubblico.

Parere 8/2019 sulla competenza di un'autorità di controllo in caso di mutamento delle circostanze relative allo stabilimento principale o unico

Adottato il 9 luglio 2019

Indice

1 Sintesi dei fatti

2 Sulla competenza del comitato ad adottare un parere in materia a norma dell'articolo 64, paragrafo 2

3 Disposizioni pertinenti

4 Parere del comitato europeo per la protezione dei dati
- 4.1 Oggetto del parere
- 4.2 Criteri applicati nel formulare il parere
- 4.3 Il parere adottato
  - 4.3.1 Trasferimento dello stabilimento principale o unico all'interno del see
  - 4.3.2 Creazione dello stabilimento principale o unico oppure trasferimento da un paese terzo nel see
  - 4.3.3 Scomparsa dello stabilimento principale o unico

5 Conclusione

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 63 e l'articolo 64, paragrafo 2, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in appresso: «RGPD»),

visto l'accordo SEE e in particolare l'allegato XI e il protocollo n. 37 dello stesso, come modificato dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018,

visto l'articolo 10 e l'articolo 22 del proprio regolamento interno del 25 maggio 2018,

considerando quanto segue:

1) Il ruolo principale del comitato europeo per la protezione dei dati (in appresso il «comitato») è garantire l'applicazione coerente dell'RGPD in tutto lo Spazio economico europeo. L'articolo 64, paragrafo 2, dell'RGPD stabilisce che qualsiasi autorità di controllo, il presidente del comitato o la Commissione può richiedere che le questioni di applicazione generale o che producono effetti in più di uno Stato membro [del SEE] siano esaminate dal comitato al fine di ottenere un parere. Il presente parere ha lo scopo di esaminare una questione di applicazione generale o che produce effetti in più di uno Stato membro del SEE.

2) Il 30 aprile 2019, le autorità di protezione dei dati di Francia e Svezia hanno chiesto al comitato di esaminare ed emettere un parere in merito al mantenimento della competenza di un'autorità nazionale in caso di mutamento delle circostanze relative allo stabilimento principale o unico.

3) Il parere del comitato è adottato a norma dell'articolo 64, paragrafo 3, dell'RGPD in combinato disposto con l'articolo 10, paragrafo 2, del regolamento interno entro otto settimane dal primo giorno lavorativo successivo alla decisione del presidente e delle autorità di controllo attestante la completezza del fascicolo. Tale periodo può essere prorogato di ulteriori sei settimane, su decisione del presidente, tenendo conto della complessità dell'argomento.

HA ADOTTATO IL SEGUENTE PARERE:

1. SINTESI DEI FATTI

1. Le autorità di protezione dei dati di Francia e Svezia hanno chiesto al comitato di esaminare la questione del mantenimento della competenza di un'autorità nazionale in caso di mutamento delle circostanze relative allo stabilimento principale o unico nonché di formulare un parere in merito.
2. Tali mutamenti possono verificarsi quando:

- uno stabilimento unico o principale viene trasferito da un paese del SEE a un altro paese del SEE;
- uno stabilimento unico o principale cessa di esistere nel territorio del SEE;
- uno stabilimento principale viene istituito nel territorio di un paese del SEE o si sposta da un paese terzo a un paese del SEE.

3. Nello specifico, le autorità di protezione dei dati di Francia e Svezia hanno formulato le seguenti domande:

- a decorrere da quando la competenza di un'autorità va considerata fissata in maniera definitiva, rendendo ininfluente ai fini della procedura qualsiasi mutamento delle circostanze dello stabilimento principale o unico?
- Si tratterebbe del momento iniziale in cui un'autorità riceve un reclamo, oppure, qualora non si basi su un reclamo, del momento in cui l'autorità inizia a esaminare un trattamento a propria discrezione?
- Si tratterebbe del momento in cui un'autorità decide di avviare un'indagine e contatta il titolare del trattamento/responsabile del trattamento?
- Si tratterebbe del momento in cui viene avviato un processo decisionale?
- Si tratterebbe del momento in cui l'autorità pronuncia una decisione ponendo così fine al caso in questione?

4. La decisione concernente la completezza del fascicolo è stata resa il 17 maggio 2019. Il termine per l'adozione del parere è stato fissato al 12 luglio.

2. SULLA COMPETENZA DEL COMITATO AD ADOTTARE UN PARERE IN MATERIA A NORMA DELL'ARTICOLO 64, PARAGRAFO 2

5. Il comitato ritiene che la questione della competenza di un'autorità nazionale in caso di mutamento delle circostanze relative allo stabilimento principale o unico costituisca una «*questione di applicazione generale*» dell'RGPD, essendovi l'evidente necessità di un'interpretazione coerente tra le autorità di protezione dei dati in merito ai limiti delle rispettive competenze. Risulta particolarmente necessario un chiarimento al fine di garantire, tra l'altro, una prassi coerente nel contesto della cooperazione conformemente all'articolo 60 dell'RGPD, dell'assistenza reciproca conformemente all'articolo 61 dell'RGPD e delle operazioni congiunte conformemente all'articolo 62 dell'RGPD.
6. In effetti, l'RGPD non contiene alcuna disposizione specifica relativa al caso in cui lo stabilimento principale o unico del titolare o del responsabile del trattamento sia istituito nel territorio di uno Stato membro del SEE e venga

trasferito, durante lo svolgimento di un procedimento, nel territorio di un altro Stato membro o al di fuori dello Spazio economico europeo, né relativa al caso in cui uno stabilimento venga creato oppure cessi di esistere nello Spazio economico europeo durante lo svolgimento di un procedimento.

7. Analogamente, le linee guida del comitato europeo per la protezione dei dati e, in particolare, quelle relative all'autorità di controllo capofila non contengono più informazioni di quelle fornite dall'RGPD in merito a tali situazioni.

8. Tuttavia, per consentire un'attuazione coerente in tutto lo Spazio economico europeo, occorre trovare un criterio obiettivo per fissare il momento a decorrere dal quale qualsiasi mutamento di circostanze non avrebbe alcun effetto sulla competenza acquisita da un'autorità. Si tratta di una tematica di notevole importanza in quanto è necessario affrontare la questione della potenziale concorrenza di competenze tra autorità di controllo. Di conseguenza è necessario chiarire le questioni sollevate non soltanto dal punto di vista della certezza del diritto, ma anche da una prospettiva operativa (trattazione di casi da parte delle autorità di protezione dei dati).

9. Per tali motivi, il comitato ritiene che le questioni sollevate dalle autorità di protezione dei dati di Francia e Svezia possano essere oggetto di un parere ai sensi dell'articolo 64, paragrafo 2.

3. DISPOSIZIONI PERTINENTI

10. L'articolo 4, paragrafo 3, del trattato sull'Unione europea recita: «*[i]n virtù del principio di leale cooperazione, l'Unione e gli Stati membri si rispettano e si assistono reciprocamente nell'adempimento dei compiti derivanti dai trattati. Gli Stati membri adottano ogni misura di carattere generale o particolare atta ad assicurare l'esecuzione degli obblighi derivanti dai trattati o conseguenti agli atti delle istituzioni dell'Unione. Gli Stati membri facilitano all'Unione l'adempimento dei suoi compiti e si astengono da qualsiasi misura che rischi di mettere in pericolo la realizzazione degli obiettivi dell'Unione*».

11. L'articolo 41, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea afferma che: «*[o]gni individuo ha diritto a che le questioni che lo riguardano siano trattate in modo imparziale, equo ed entro un termine ragionevole dalle istituzioni e dagli organi dell'Unione*».

12. L'articolo 51, paragrafo 1, dell'RGPD stabilisce il mandato legale delle autorità di protezione dei dati, che consiste nel sorvegliare l'applicazione dell'RGPD al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dello Spazio economico europeo.

13. Gli articoli 55, 57 e 58 specificano la competenza, i compiti e i poteri di ciascuna autorità di protezione dei dati[1].

14. L'articolo 56 prevede il meccanismo dello «*sportello unico*», una norma procedurale secondo la quale viene assegnato un ruolo specifico a un'autorità di controllo capofila, definita come l'autorità sul cui territorio il titolare o il responsabile del trattamento hanno il proprio stabilimento principale o unico[2].

15. Il capo VII dell'RGPD, intitolato «Cooperazione e coerenza», definisce i diversi modi in cui le autorità di protezione dei dati cooperano per contribuire a un'applicazione coerente dell'RGPD. Le disposizioni pertinenti sono contenute in particolare nell'articolo 60 dell'RGPD, che prevede la cooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate[3]. Analogamente, ai sensi degli articoli 61 e 62 dell'RGPD, le autorità di vigilanza si prestano assistenza reciproca e, se del caso, conducono operazioni congiunte, comprese le indagini congiunte e le misure di contrasto congiunte.

4. PARERE DEL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

4.1 OGGETTO DEL PARERE

16. Nel contesto del presente parere il comitato ritiene che le questioni vertano principalmente su violazioni di natura continuativa o continuata in ragione del fatto che, affinché si verifichi un mutamento delle circostanze relative allo stabilimento principale o unico, le violazioni devono essere commesse lungo un certo lasso di tempo. Una violazione «continuativa» è un'azione (o un'omissione) che dura per un certo lasso di tempo mentre una violazione «continuata» è un illecito consistente in diversi atti che contengono tutti gli elementi dello stesso (o di un analogo) atto illecito commessi nell'arco di un certo periodo di tempo (*Corte europea dei diritti dell'uomo, Grande Camera, causa Rohlena/Repubblica ceca, n. 59552/08*).

4.2 CRITERI APPLICATI NEL FORMULARE IL PARERE

17. Il comitato europeo per la protezione dei dati sottolinea che le norme dell'RGPD sulla distribuzione delle competenze tra le diverse autorità degli Stati membri interessati e il concetto di autorità capofila si basano su una cooperazione intensa e fluida tra le autorità di controllo. Questo nuovo livello di cooperazione deriva dal fatto che l'RGPD è attualmente il quadro giuridico comune per la protezione dei dati e pertanto le autorità di controllo non dovrebbero avere alcun dubbio sulla sua applicazione coerente e rapida né incontrare alcun ostacolo in merito. Di conseguenza, nel valutare la risposta corretta ai quesiti posti, un punto di partenza ineliminabile è da individuarsi nella cooperazione efficace delle autorità di controllo basata sulla fiducia reciproca.

18. Per consentire un'attuazione coerente in tutto lo Spazio economico europeo, occorre trovare un criterio obiettivo per cristallizzare il momento a partire dal quale ogni eventuale mutamento di circostanze non esplicherebbe alcun effetto sulla competenza acquisita da un'autorità. Tale criterio dovrebbe soddisfare tre obiettivi:

- garantire tanto al titolare quanto al responsabile del trattamento un grado sufficiente di certezza del diritto e prevedibilità, obiettivo dichiarato nell'RGPD e in particolare al considerando 13;
- tenere conto delle considerazioni relative alla buona amministrazione, garan-

tendo l'efficienza e l'efficacia delle azioni intraprese dalle autorità (cfr. in particolare l'articolo 41 della Carta dei diritti fondamentali dell'Unione europea e i considerando 11 e 13 dell'RGPD) ed evitando qualsiasi uso improprio del meccanismo dello sportello unico sotto forma di una scelta opportunistica del foro («*forum shopping*») o di un passaggio da un foro all'altro («*forum hopping*»);

- limitare il rischio di concorrenza delle competenze tra autorità.

19. L'articolo 55, paragrafo 1, e il considerando 122 dell'RGPD stabiliscono i principi generali concernenti la competenza delle autorità di controllo secondo i quali ogni autorità di controllo è «*competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti a norma del presente regolamento nel territorio del rispettivo Stato membro*». Tuttavia, l'articolo 56, paragrafo 1, e il considerando 124 contengono una norma imperativa e prevedono che l'autorità di controllo dello stabilimento principale o unico del titolare o del responsabile del trattamento sia competente a svolgere il ruolo di autorità di controllo capofila per il trattamento transfrontaliero svolto da tale titolare o responsabile del trattamento.

20. L'articolo 56, paragrafo 1, costituisce una *lex specialis* e, in quanto tale, prevale ogniqualvolta si verifichi una situazione di trattamento che soddisfi le condizioni ivi specificate, come quella in cui esista uno stabilimento principale o unico nell'UE che sia responsabile di attività di trattamento transfrontaliero e sia coinvolto in un reclamo/in una presunta violazione rilevata o segnalata. Di conseguenza, la competenza dell'autorità di controllo capofila per la gestione di un caso deriva dall'esistenza dello stabilimento principale o unico del titolare o del responsabile del trattamento nel territorio del proprio Stato membro nel contesto di un'attività di trattamento transfrontaliero. Se tale stabilimento principale o unico viene trasferito successivamente all'avvio di un procedimento dinanzi all'autorità di controllo capofila o su iniziativa di quest'ultima, e se il nuovo stabilimento principale o unico soddisfa le condizioni per essere considerato tale, allora il titolare o il responsabile del trattamento avranno il diritto di fare affidamento su un nuovo interlocutore unico ai sensi dell'articolo 56, paragrafi 1 e 6, ossia la nuova autorità di controllo capofila dello Stato membro del nuovo stabilimento principale o unico.

21. Il cambiamento del ruolo di autorità di controllo capofila non significa che l'autorità di controllo iniziale non fosse competente ad agire nel momento in cui lo ha fatto e, pertanto, tale circostanza non priva retroattivamente di base giuridica le operazioni già svolte dall'autorità capofila iniziale. L'autorità di controllo precedentemente competente aveva piena giurisdizione quando lo stabilimento principale o unico era situato sul suo territorio. Di conseguenza, gli atti compiuti conservano il loro valore e gli elementi di prova e le informazioni raccolti dalla precedente autorità di controllo capofila possono essere utilizzati da quella divenuta successivamente competente.

22. Questa soluzione aumenta le possibilità che l'autorità preposta alla decisione abbia il potere di dare esecuzione alla stessa. In effetti, la nuova autorità di controllo capofila è in grado di dare esecuzione alla decisione che renderà, in quanto vi è uno stabilimento del titolare o del responsabile del trattamento nel suo territorio, circostanza questa in linea con il principio di efficace applicazione di cui al considerando 11 dell'RGPD.

23. Inoltre, questa soluzione offre il vantaggio di ridurre il rischio che due (o più) autorità si considerino capofila per la medesima violazione o, al contrario, che nessuna autorità si consideri capofila. In effetti, il criterio dell'adozione di una decisione definitiva è relativamente immediato ed è abbastanza semplice stabilire se sia soddisfatto.

24. In ogni caso, è opportuno sottolineare che, in caso di variazione dell'autorità di controllo capofila, si applicherà la procedura di cooperazione di cui all'articolo 60 e la nuova autorità di controllo capofila sarà tenuta a cooperare con la precedente e con le altre autorità di controllo interessate al fine del raggiungimento del consenso, quanto meno se la precedente autorità di controllo capofila continua a essere un'autorità di controllo interessata. Nella pratica ciò significa che la nuova autorità di controllo capofila dovrà presentare un progetto di decisione alla precedente autorità di controllo capofila (e a tutte le altre autorità di controllo interessate) e quest'ultima, così come ogni altra autorità di controllo interessata, avrà la possibilità di esprimere un'obiezione pertinente e motivata. Inoltre, la precedente autorità di controllo capofila potrà partecipare allo svolgimento delle indagini nel contesto di operazioni congiunte ai sensi dell'articolo 62 qualora soddisfi i criteri di cui all'articolo 4, paragrafo 22.

25. Il fatto che sia stata adottata una decisione definitiva nel contesto di una procedura di cooperazione avviata ai sensi dell'articolo 60 dell'RGPD deve essere tenuto in debito conto, in particolare assicurando che l'autorità di controllo precedente (capofila) sia coinvolta in eventuali fasi successive da parte dell'autorità di controllo capofila subentrata successivamente, in maniera da evitare di compromettere l'efficacia della procedura amministrativa e/o di introdurre ulteriori ritardi nell'individuazione dei rimedi pertinenti (anche conformemente all'articolo 41 della Carta dei diritti fondamentali dell'Unione europea).

26. Infine, occorre osservare che per impedire una scelta opportunistica del foro e garantire un'efficace protezione degli interessati, il trasferimento dello stabilimento principale deve essere efficace e comprovato dal titolare del trattamento (cfr. il documento WP244, intitolato «*Linee guida per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento*», adottato il 13 dicembre 2016 dal Gruppo dell'articolo 29 per la tutela dei dati, pag. 8). Il concetto stesso di stabilimento principale indica che la sua definizione per l'impresa non costituisce un mero atto momentaneo o burocratico, bensì un'operazione concreta, attuata secondo propositi duraturi. Di conseguenza le autorità di controllo dovrebbero esercitare un controllo effettivo sulla nozione di stabilimento principale al fine di ridurre il rischio che i titolari o i responsabili del trattamento modifichino artificiosamente il rispettivo stabilimento principale al fine di sostituire l'autorità competente per l'esame del caso.

4.3 IL PARERE ADOTTATO

4.3.1 TRASFERIMENTO DELLO STABILIMENTO PRINCIPALE O UNICO ALL'INTERNO DEL SEE

27. Fatte salve le considerazioni di cui sopra, si ritiene che il trasferimento dello stabilimento principale nel territorio di un altro Stato membro del SEE durante lo svolgimento di un procedimento privi la prima autorità della sua competenza originaria in qualità di capofila nel momento in cui tale mutamento di sede diventa effettivo, senza tuttavia privare retrospettivamente di base giuridica le operazioni già svolte da tale prima autorità.
28. Qualsiasi procedimento pendente sarà trasferito all'autorità di controllo dello Stato nel quale si trova lo stabilimento principale. Tale autorità di controllo diventerà l'autorità di controllo capofila e il procedimento proseguirà conformemente alle norme di cui all'articolo 60, in cooperazione con l'autorità di controllo interessata di cui all'articolo 4, paragrafo 22.
29. Si ritiene che il trasferimento dello stabilimento principale o unico all'interno del SEE privi la prima autorità del suo ruolo originario di autorità di controllo capofila nel momento in cui tale mutamento diventa efficace ed è comprovato. Come già menzionato, sarà applicabile la procedura di cooperazione di cui all'articolo 60 e la nuova autorità di controllo capofila sarà tenuta a cooperare con quella precedente e con le altre autorità di controllo interessate al fine di raggiungere un consenso.

4.3.2 CREAZIONE DELLO STABILIMENTO PRINCIPALE O UNICO OPPURE TRASFERIMENTO DA UN PAESE TERZO NEL SEE

30. Il comitato europeo per la protezione dei dati ritiene che la competenza ad agire in qualità di autorità capofila possa essere trasferita a un'altra autorità di controllo fino a quando l'autorità di controllo capofila non ha adottato una decisione definitiva. Di conseguenza, la creazione di uno stabilimento principale o unico oppure il suo trasferimento da un paese terzo nel SEE (nel contesto di un procedimento inizialmente avviato senza cooperazione) durante lo svolgimento di un procedimento consentirà al titolare del trattamento di beneficiare del meccanismo dello sportello unico.
31. Qualsiasi procedimento pendente (necessariamente un procedimento non soggetto a cooperazione data l'assenza iniziale di uno stabilimento principale nel SEE) sarà trasferito all'autorità di controllo dello Stato nel quale si trova lo stabilimento principale. Tale autorità di controllo diventerà l'autorità di controllo capofila e il procedimento proseguirà conformemente alle norme di cui all'articolo 60, in cooperazione con l'autorità di controllo interessata di cui all'articolo 4, paragrafo 22.
32. Si ritiene che la creazione di uno stabilimento principale o unico oppure il suo trasferimento da un paese terzo privi la prima autorità della sua competenza originaria dovuta alla presentazione del reclamo dinanzi a essa nel

momento in cui tale mutamento di circostanze diventa efficace ed è comprovato. Come già menzionato, sarà applicabile la procedura di cooperazione di cui all'articolo 60 e la nuova autorità di controllo capofila sarà tenuta a cooperare con quella precedente e con le altre autorità di controllo interessate con l'obiettivo di raggiungere un consenso.

4.3.3 SCOMPARSA DELLO STABILIMENTO PRINCIPALE O UNICO

33. Il comitato europeo per la protezione dei dati ritiene che la competenza ad agire in qualità di autorità capofila possa essere trasferita a un'altra autorità di controllo fino a quando l'autorità di controllo capofila non abbia adottato una decisione definitiva. Di conseguenza, la scomparsa dello stabilimento principale o unico durante lo svolgimento di un procedimento (in ragione del trasferimento dello stabilimento principale al di fuori dal territorio del SEE oppure del suo scioglimento) determinerà l'impossibilità per il titolare del trattamento di beneficiare del meccanismo dello sportello unico.

34. Nel caso in cui lo stabilimento cessi di esistere nel territorio del suo Stato membro, la precedente autorità di controllo capofila rimane competente così come qualsiasi altra autorità di controllo interessata ai sensi dell'articolo 4, paragrafo 22, dell'RGPD. Poiché il trattamento non può più essere considerato transfrontaliero, il principio di cooperazione decade e ogni autorità interessata riacquista piena giurisdizione.

5. CONCLUSIONE

35. In conclusione, il comitato ritiene che la competenza ad agire in qualità di autorità di controllo capofila possa essere trasferita a un'altra autorità di controllo in caso di mutamento documentato delle circostanze relative allo stabilimento principale o unico di un titolare o di un responsabile del trattamento fino all'adozione di una decisione definitiva da parte di tale autorità di controllo.

Per il comitato europeo per la protezione dei dati
La presidente

(Andrea Jelinek)

NOTE

[1] A questo proposito occorre ricordare che il considerando 11 dell'RGPD prevede quanto segue: «*[u]n'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri*». Il considerando 13 dell'RGPD afferma che uno degli obiettivi del regolamento consiste nel «*[garantire] certezza del diritto e trasparenza agli operatori economici [...] e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri*». Infine, conformemente al considerando 122, «*[o]gni autorità di controllo dovrebbe avere la competenza, nel territorio del proprio Stato membro, a esercitare i poteri e ad assolvere i compiti a essa attribuiti a norma del presente regolamento*».

[2] il considerando 124 dispone che: «*[q]ualora il trattamento dei dati personali abbia luogo nell'ambito delle attività di uno stabilimento di un titolare del trattamento o di un responsabile del trattamento nell'Unione e il titolare del trattamento o il responsabile del trattamento sia stabilito in più di uno Stato membro o qualora il trattamento effettuato nell'ambito delle attività dello stabilimento unico di un titolare del trattamento o responsabile del trattamento nell'Unione incida o possa verosimilmente incidere in modo sostanziale su interessati in più di uno Stato membro, l'autorità di controllo dello stabilimento principale del titolare del trattamento o del responsabile del trattamento o dello stabilimento unico del titolare del trattamento o del responsabile del trattamento dovrebbe fungere da autorità capofila*».

[3] Ciò è confermato dai considerando da 123 a 126 e 130. Più specificamente, secondo il considerando 125 «*[...] [n]ella sua qualità di autorità capofila, l'autorità di controllo dovrebbe coinvolgere e coordinare strettamente le autorità di controllo interessate nel processo decisionale*». Il considerando 126 afferma che «*[l]a decisione dovrebbe essere adottata congiuntamente dall'autorità di controllo capofila e dalle autorità di controllo interessate e dovrebbe essere rivolta allo stabilimento principale o unico del titolare del trattamento o del responsabile del trattamento [...]*».

Linee guida 9/2020 sull'obiezione pertinente e motivata ai sensi del regolamento (UE) 2016/679 Versione 2.0

Adottate il 9 marzo 2021

Cronologia delle versioni

Versione 1.0	8 ottobre 2020	Adozione delle linee guida per la conultazione pubblica
Versione 2.0	9 marzo 2021	Adozione delle linee guida dopo la consultazione pubblica

Indice

1 Informazioni generali

2 Condizioni per un'obiezione "pertinente e motivata"
- 2.1 "Pertinente"
- 2.2 "Motivata"

3 Contenuto dell'obiezione
- 3.1 Sussistenza di una violazione del GDPR e/o conformità al GDPR dell'azione prevista
  - 3.1.1 Sussistenza di una violazione del GDPR
  - 3.1.2 Conformità al GDPR dell'azione prevista nel progetto di decisione in relazione al titolare del trattamento o al responsabile del trattamento
- 3.2 Rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione
  - 3.2.1 Significato di "rilevanza dei rischi"
  - 3.2.2 Rischi per i diritti e le libertà degli interessati
  - 3.2.3 Rischi per la libera circolazione dei dati personali all'interno dell'Unione

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI,

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo n. 37, modificati dalla decisione del comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

visti gli articoli 12 e 22 del proprio regolamento interno,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

1. INFORMAZIONI GENERALI

1. Nell'ambito del meccanismo di cooperazione previsto dal regolamento generale sulla protezione dei dati ("GDPR"), le autorità di controllo hanno il dovere di scambiarsi "tutte le informazioni utili" e di cooperare "nell'impegno per raggiungere un consenso"[2]. Tale dovere di cooperazione si applica a tutte le fasi della procedura, dall'avvio del caso e nel corso dell'intero processo decisionale. Il raggiungimento di un accordo sull'esito del caso rappresenta pertanto il fine ultimo di tutta la procedura stabilita all'articolo 60 GDPR. Ove non si raggiunga un consenso tra le autorità di controllo, l'articolo 65 GDPR conferisce al Comitato europeo per la protezione dei dati ("Comitato" o "EDPB") il potere di adottare decisioni vincolanti. Tuttavia lo scambio di informazioni e la consultazione tra l'autorità di controllo capofila e le autorità di controllo interessate consente spesso di trovare un accordo nelle fasi iniziali del caso.
2. A norma dell'articolo 60, paragrafi 3 e 4, GDPR, l'autorità di controllo capofila è tenuta a trasmettere un progetto di decisione alle autorità di controllo interessate, le quali possono sollevare un'obiezione pertinente e motivata entro un termine specifico (quattro settimane)[3]. Quando l'autorità di controllo capofila riceve un'obiezione pertinente e motivata può scegliere tra due opzioni. Ove non dia seguito all'obiezione pertinente e motivata o ritenga l'obiezione non pertinente o non motivata, sottopone la questione al Comitato europeo per la protezione dei dati mediante il meccanismo di coerenza. Se, al contrario, l'autorità di controllo capofila dà seguito all'obiezione e presenta un progetto di decisione riveduto, le autorità di controllo interessate possono esprimere un'obiezione pertinente e motivata entro un termine di due settimane.
3. Se l'autorità di controllo capofila non dà seguito all'obiezione o la rigetta in quanto non pertinente o non motivata e quindi sottopone la questione al Comitato a norma dell'articolo 65, paragrafo 1, lettera a), GDPR, il Comitato è tenuto ad adottare una decisione vincolante che stabilisce se l'obiezione sia "pertinente e motivata" e, in caso affermativo, definisce tutte le questioni oggetto dell'obiezione.
4. Pertanto, uno degli elementi chiave che denota l'assenza di consenso tra l'autorità di controllo capofila e le autorità di controllo interessate è il concetto di "obiezione pertinente e motivata". Il presente documento intende fornire orientamenti rispetto a tale concetto e definire un'interpretazione condivisa dei termini "pertinente e motivata", compresi gli elementi da tenere in considerazione nel valutare se un'obiezione "dimostr[i] chiaramente la rilevanza dei rischi posti dal progetto di decisione" (articolo 4, punto 24, GDPR).
5. Ai sensi dell'articolo 4, punto 24, GDPR per "obiezione pertinente e motivata" s'intende: "*un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione*".

6. Questo concetto funge da **soglia** ogniqualvolta le autorità di controllo interessate intendano sollevare un'obiezione a un progetto di decisione (riveduto) che deve essere adottato dall'autorità di controllo capofila a norma dell'articolo 60 GDPR. Dato che l'incertezza rispetto a "ciò che costituisce obiezione pertinente e motivata" può generare incomprensioni e condurre a un'applicazione incoerente da parte delle autorità di controllo, il legislatore dell'UE ha suggerito che l'EDPB pubblichi linee guida su questo concetto (parte finale del considerando 124 GDPR).

7. Affinché soddisfi il livello di soglia stabilito all'articolo 4, punto 24, GDPR, quanto presentato da un'autorità di controllo interessata dovrebbe, in linea di principio, menzionare in modo esplicito ogni elemento della definizione per ogni obiezione specifica. Pertanto, **lo scopo dell'obiezione è, innanzitutto, indicare come e perché, secondo l'autorità di controllo interessata, il progetto di decisione non affronti in modo adeguato la situazione di violazione del GDPR e/o non preveda un'azione appropriata nei confronti del titolare del trattamento o del responsabile del trattamento, alla luce della dimostrazione dei rischi che tale progetto di decisione, qualora non sia modificato, comporterebbe per i diritti e per le libertà degli interessati e, ove applicabile, per la libera circolazione dei dati personali all'interno dell'Unione**. L'obiezione presentata da un'autorità di controllo interessata dovrebbe indicare ogni parte del progetto di decisione ritenuta carente, errata o mancante di elementi necessari, con riferimenti ad articoli/paragrafi specifici o altre indicazioni chiare, e dovrebbe dimostrare i motivi per cui tali aspetti siano considerati "pertinenti", come approfondito di seguito. Le proposte di modifica avanzate nell'obiezione dovrebbero essere intese a porre rimedio a tali potenziali errori.

8. In effetti, **il livello di dettaglio dell'obiezione e la profondità dell'analisi svolta in essa possono dipendere dal livello di dettaglio del contenuto del progetto di decisione e dal grado di partecipazione dell'autorità di controllo interessata** al processo che conduce al progetto di decisione emesso dell'autorità di controllo capofila. Pertanto, il criterio relativo all'"obiezione pertinente e motivata" si fonda sul presupposto che l'autorità di controllo capofila rispetti l'obbligo di scambiare tutte le informazioni utili[4], in modo da consentire alle autorità di controllo interessate di avere una conoscenza approfondita del caso in questione e di presentare un'obiezione solida e ben motivata. A tale scopo è opportuno tenere presente che ogni misura giuridicamente vincolante adottata dalle autorità di controllo dovrebbe "precisare i motivi della misura" (cfr. considerando 129 GDPR). Ne consegue che il livello del coinvolgimento dell'autorità di controllo interessata nel processo che sfocia nel progetto di decisione da parte dell'autorità di controllo capofila, se non consente una conoscenza sufficiente di tutti gli aspetti del caso, può costituire un fattore di flessibilità rispetto al livello di dettaglio richiesto per l'obiezione pertinente e motivata.

9. L'EDPB desidera sottolineare in primo luogo che le autorità di controllo coinvolte (l'autorità di controllo capofila e le autorità di controllo interessate) dovrebbero adoperarsi per eliminare qualsiasi carenza nel processo di ricerca

del consenso, in modo tale da pervenire a un progetto di decisione consensuale. Pur ammettendo che sollevare un'obiezione non è il modo migliore per porre rimedio a un insufficiente livello di cooperazione nelle fasi precedenti della procedura dello sportello unico, l'EDPB riconosce che si tratta di un'opzione a disposizione delle autorità di controllo interessate. Tale opzione dovrebbe essere considerata come soluzione di ultima istanza anche allo scopo di porre rimedio alle (presunte) carenze in termini di coinvolgimento delle autorità di controllo interessate da parte dell'autorità di controllo capofila nel processo che avrebbe dovuto condurre a un progetto di decisione consensuale, anche per quanto concerne l'analisi giuridica e l'ambito delle indagini svolte dall'autorità di controllo capofila sul caso in questione.

10. Il GDPR impone all'autorità di controllo interessata di giustificare la propria posizione rispetto al progetto di decisione dell'autorità di controllo capofila, presentando un'obiezione che sia "pertinente" e "motivata". È fondamentale tenere presente che i due requisiti, "motivata" e "pertinente", devono essere considerati **cumulativi**, ossia entrambi devono essere soddisfatti[5]. Pertanto, l'articolo 60, paragrafo 4, impone all'autorità di controllo capofila di sottoporre la questione al meccanismo di coerenza dell'EDPB se ritiene che l'obiezione non soddisfi anche solo uno dei due requisiti[6].

11. L'EDPB consiglia vivamente alle autorità di controllo di sollevare le proprie obiezioni e di scambiare informazioni attraverso il sistema di informazione e di comunicazione istituito per lo scambio di informazioni tra le autorità di controllo[7]. Le obiezioni e le informazioni dovrebbero essere chiaramente indicate come tali utilizzando le funzioni e gli strumenti specifici previsti a tale scopo.

2. CONDIZIONI PER UN'OBIEZIONE "PERTINENTE E MOTIVATA"

2.1 "PERTINENTE"

12. Affinché l'obiezione sia considerata "pertinente", deve esserci un **collegamento diretto tra l'obiezione e il contenuto del progetto di decisione in questione**[8]. Più specificamente, l'obiezione deve **riferirsi alla sussistenza di una violazione del GDPR oppure alla conformità al GDPR dell'azione prevista in relazione al titolare del trattamento o al responsabile del trattamento**.

13. Di conseguenza, l'obiezione sollevata soddisfa il requisito dell'essere "pertinente" quando comporti, ove accolta, una modifica che conduca a **una conclusione diversa** riguardo alla sussistenza o meno di una violazione del GDPR, oppure alla conformità o meno al GDPR dell'azione prevista in relazione al titolare del trattamento o al responsabile del trattamento, proposta dall'autorità di controllo capofila. Tra il contenuto dell'obiezione e tale conclusione potenzialmente diversa deve esserci sempre un nesso, come spiegato di seguito. Benché sia possibile che un'obiezione esprima un dissenso in merito a entrambi gli elementi, l'esistenza di uno solo di essi sarebbe sufficiente a soddisfare le condizioni di un'obiezione pertinente.

14. Un'obiezione dovrebbe essere considerata pertinente soltanto se riguarda specifici elementi di fatto o di diritto del progetto di decisione dell'autorità di controllo capofila. In tale contesto non può essere considerata pertinente un'obiezione che sollevi preoccupazioni o osservazioni astratte o generiche. Analogamente, dissensi di minore entità sulla formulazione o sull'analisi giuridica, che non riguardino né l'eventuale sussistenza di una violazione né la conformità al GDPR dell'azione prevista in relazione al titolare del trattamento o al responsabile del trattamento, non dovrebbero essere considerati pertinenti.
15. L'analisi giuridica a supporto delle conclusioni dell'autorità di controllo capofila nel progetto di decisione può essere oggetto di un'obiezione, ma solo nella misura in cui tale analisi sia correlata alla conclusione sulla sussistenza o meno di una violazione del GDPR, sulla correttezza o meno dell'individuazione della violazione del GDPR oppure sulla conformità o meno al GDPR dell'azione prevista, e nella misura in cui la soglia di cui all'articolo 4, punto 24, sia stata raggiunta nella sua interezza come descritto nel presente documento.

2.2 "MOTIVATA"

16. Affinché l'obiezione sia "motivata"[9] occorre che essa chiarisca e argomenti il **motivo per cui si propone una modifica della decisione** (vale a dire gli errori di fatto/di diritto del progetto di decisione dell'autorità di controllo capofila). Deve inoltre dimostrare **in che modo la modifica condurrebbe a una diversa conclusione** sulla sussistenza o meno di una violazione del GDPR oppure sulla conformità o meno al GDPR dell'azione prevista in relazione al titolare del trattamento o al responsabile del trattamento.
17. L'autorità di controllo interessata dovrebbe fornire una motivazione solida e fondata a sostegno della propria obiezione, in particolare circostanziando **gli argomenti giuridici** (invocando il diritto dell'Unione e/o il diritto nazionale pertinente, tra cui, ad esempio, disposizioni giuridiche, giurisprudenza, linee guida) **o gli elementi fattuali**, se del caso. L'autorità di controllo interessata dovrebbe presentare i fatti che presumibilmente condurrebbero a una conclusione diversa in merito alla violazione del GDPR da parte del titolare o del responsabile del trattamento, oppure l'aspetto del progetto di decisione che, a suo parere, è carente/errato.
18. Un'obiezione inoltre è "motivata" nella misura in cui **"dimostra chiaramente" la rilevanza dei rischi posti dal progetto di decisione**, come descritto di seguito nella sezione 3.2. A tal fine, l'obiezione deve presentare argomenti o giustificazioni riguardanti le conseguenze derivanti dalla mancata modifica della decisione nei termini proposti nell'obiezione e in che modo tali conseguenze potrebbero comportare rischi rilevanti per i diritti e le libertà fondamentali degli interessati e, ove applicabile, per la libera circolazione dei dati personali all'interno dell'Unione.
19. Affinché un'obiezione sia adeguatamente motivata, dovrebbe essere **coerente, chiara, precisa e dettagliata nello spiegare i motivi dell'obiezione** stessa. Essa dovrebbe esporre, in modo chiaro e preciso, gli **elementi essenziali**

sui quali l'autorità di controllo interessata ha fondato la propria valutazione e il **nesso tra le conseguenze previste del progetto di decisione** (se fosse emesso senza modifiche) **e la rilevanza dei rischi attesi per i diritti e le libertà fondamentali degli interessati e, ove applicabile, per la libera circolazione dei dati personali all'interno dell'Unione**. L'autorità di controllo interessata dovrebbe inoltre precisare chiaramente quali sono le parti del progetto di decisione su cui dissente. Nei casi in cui l'obiezione si basi sull'opinione che l'autorità di controllo capofila non abbia pienamente indagato un fatto importante del caso, o un'ulteriore violazione del GDPR, sarebbe sufficiente che l'autorità di controllo interessata presentasse tali argomenti in maniera concludente e circostanziata.

20. L'autorità di controllo interessata deve fornire tutte le informazioni (fatti, documenti, argomenti giuridici) sulle quali si basa, in modo da presentare un'argomentazione efficace. Ciò è fondamentale al fine di circoscrivere l'ambito della (potenziale) controversia. Questo significa che, **in linea di principio, l'autorità di controllo interessata dovrebbe mirare a presentare un'obiezione pertinente e motivata in un'unica soluzione**, fondata su tutti gli argomenti di fatto e di diritto nei termini sopra descritti. Tuttavia **entro il termine stabilito all'articolo 60, paragrafo 4, GDPR, l'autorità di controllo interessata può fornire informazioni supplementari riguardo all'obiezione sollevata e a suo sostegno, tenendo presente la necessità di soddisfare i requisiti concernenti il suo essere "pertinente e motivata"**.

> **Esempio 1**
>
> L'autorità di controllo interessata trasmette un'obiezione formale, ma alcuni giorni più tardi fornisce all'autorità di controllo capofila ulteriori informazioni sui fatti relativi al caso in questione attraverso il sistema di informazione e comunicazione. L'autorità di controllo capofila può prendere in considerazione tali informazioni soltanto se sono state presentate entro il termine stabilito dall'articolo 60, paragrafo 4, GDPR.

21. Laddove possibile, come buona pratica, l'obiezione dovrebbe contenere **una proposta di riformulazione** che, secondo l'autorità di controllo interessata, permetta di porre rimedio alle presunte lacune del progetto di decisione. Ciò può consentire di chiarire meglio l'obiezione nel contesto pertinente.

3. CONTENUTO DELL'OBIEZIONE

22. L'oggetto dell'obiezione può riguardare la sussistenza o meno di una violazione del GDPR e/o la conformità o meno al GDPR dell'azione prevista in relazione al titolare del trattamento o al responsabile del trattamento. Il contenuto dipenderà dal progetto di decisione emesso dall'autorità di controllo capofila e dalle circostanze del caso.

23. L'obiezione sollevata dall'autorità di controllo interessata dovrà inoltre dimostrare chiaramente la rilevanza dei rischi posti dal progetto di decisio-

ne riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione. La sussistenza di una violazione e/o la non conformità al GDPR dell'azione prevista dovrebbero essere valutate alla luce della rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà degli interessati e, ove applicabile, alla libera circolazione dei dati personali qualora esso non fosse modificato.

3.1 SUSSISTENZA DI UNA VIOLAZIONE DEL GDPR E/O CONFORMITÀ AL GDPR DELL'AZIONE PREVISTA

3.1.1 SUSSISTENZA DI UNA VIOLAZIONE DEL GDPR

24. Nel primo caso, il contenuto dell'obiezione consisterà in una divergenza di vedute tra l'autorità di controllo interessata e l'autorità di controllo capofila riguardo al quesito se, alla luce dei fatti in questione, le attività e le operazioni di trattamento effettuate dal titolare o dal responsabile del trattamento abbiano comportato una violazione o più violazioni del GDPR, e nello specifico di quale o quali violazioni si tratti.
25. In questo contesto il termine "violazione" dovrebbe intendersi come "violazione di una data disposizione del GDPR". Pertanto, le obiezioni al progetto di decisione sollevate dall'autorità di controllo interessata devono essere giustificate e motivate mediante riferimenti agli elementi probatori e fattuali scambiati tra l'autorità di controllo capofila e le autorità di controllo interessate (le "informazioni utili" di cui all'articolo 60 GDPR). Tali requisiti dovrebbero applicarsi a ogni specifica violazione e a ogni specifica disposizione in questione.

Esempio 2

Il progetto di decisione afferma che il titolare del trattamento ha violato gli articoli 6, 7 e 14 GDPR. L'autorità di controllo interessata dissente in merito alla sussistenza di una violazione degli articoli 7 e 14 e ritiene che sussista una violazione anche dell'articolo 13 GDPR.

Esempio 3

L'autorità di controllo interessata sostiene che l'autorità di controllo capofila non ha preso in considerazione il fatto che la deroga relativa alle attività a carattere domestico non si applica ad alcune operazioni di trattamento effettuate dal titolare del trattamento, le quali comportano l'uso di telecamere a circuito chiuso, e pertanto non sussiste alcuna violazione del GDPR. Per motivare la propria obiezione, l'autorità di controllo interessata fa riferimento all'articolo 2, paragrafo 2, lettera c), GDPR, alle linee guida 3/2019 dell'EDPB sul trattamento dei dati personali attraverso dispositivi video e alla sentenza della Corte di giustizia dell'11 dicembre 2014, Ryneš, C-212/13.

26. Un'obiezione sulla sussistenza di una violazione del GDPR può rilevare anche una divergenza di vedute in merito alle conclusioni da trarre dai risultati dell'indagine. L'obiezione, ad esempio, può affermare che dai risultati dell'indagine si evince la violazione di una disposizione del GDPR diversa (e/o ulteriore) rispetto a quelle già esaminate nel progetto di decisione dell'autorità di controllo capofila. Tuttavia, è meno probabile che ciò accada quando da parte dell'autorità di controllo capofila è stato debitamente osservato l'obbligo di cooperare e di scambiare tutte le informazioni utili con le autorità di controllo interessate, a norma dell'articolo 60, paragrafo 1, GDPR, nel periodo antecedente alla trasmissione del progetto di decisione.

27. In determinate circostanze, un'obiezione potrebbe addirittura evidenziare lacune nel progetto di decisione che giustificano lo svolgimento di ulteriori indagini da parte dell'autorità di controllo capofila. Ad esempio, se l'indagine condotta dall'autorità di controllo capofila omette in modo ingiustificato di considerare alcune questioni sollevate dal reclamo o conseguenti alla violazione riferita da un'autorità di controllo interessata, è possibile sollevare un'obiezione pertinente e motivata fondata sul fatto che l'autorità di controllo capofila ha omesso di trattare adeguatamente il reclamo e di tutelare i diritti dell'interessato. A tale proposito è opportuno fare una distinzione tra, da un lato, le indagini svolte d'ufficio e, dall'altro, le indagini avviate sulla base di reclami o segnalazioni in merito a eventuali violazioni e trasmessi dalle autorità di controllo interessate. Nelle procedure avviate sulla base di un reclamo o di una violazione segnalata da un'autorità di controllo interessata, l'ambito della procedura (ossia gli aspetti del trattamento dei dati che sono potenzialmente oggetto di violazione) dovrebbe essere definito in base al contenuto del reclamo o della segnalazione trasmessa dall'autorità di controllo interessata. In altri termini, l'ambito della procedura dovrebbe essere definito in base agli aspetti oggetto del reclamo o della segnalazione. Per le indagini svolte d'ufficio, l'autorità di controllo capofila e le autorità di controllo interessate dovrebbero cercare un consenso in merito all'ambito della procedura (ossia gli aspetti del trattamento sottoposti ad esame) prima del suo avvio formale. Ciò vale anche qualora un'autorità di controllo che sta esaminando un reclamo o una segnalazione proveniente da un'altra autorità di controllo ritenga che sia necessario avviare anche un'indagine d'ufficio per affrontare questioni di compliance che hanno natura sistemica ed esulano, quindi, dallo specifico reclamo o dalla specifica segnalazione.

28. Come già affermato, sollevare un'obiezione dovrebbe essere considerata una soluzione di ultima istanza per porre rimedio a un coinvolgimento delle autorità di controllo interessate ritenuto insufficiente nelle fasi precedenti della procedura. Il sistema concepito dal legislatore sembra indicare che le autorità di controllo competenti dovrebbero definire consensualmente l'ambito dell'indagine in una fase precedente della procedura.

29. L'oggetto di un'obiezione collegata alla sussistenza di una violazione può consistere anche nell'insufficiente descrizione del caso in questione o nell'insufficienza degli elementi fattuali oppure nella carenza o insufficienza delle valutazioni o dell'analisi svolte (cosicché le conclusioni dell'autorità di con-

trollo capofila nel progetto di decisione non sono adeguatamente supportate dalla valutazione svolta e dagli elementi probatori presentati, come disposto all'articolo 58 GDPR). Ciò a condizione che sia pienamente rispettata la soglia di cui all'articolo 4, punto 24, GDPR e che sia possibile individuare un nesso tra tale analisi asseritamente insufficiente e la conclusione relativa alla sussistenza di una violazione/l'azione prevista.

30. Un'obiezione pertinente e motivata può riguardare aspetti procedurali qualora essi si riferiscano a situazioni in cui l'autorità di controllo capofila abbia presumibilmente ignorato i requisiti procedurali imposti dal GDPR pregiudicando in tal modo le conclusioni raggiunte nel progetto di decisione.

Esempio 4

L'autorità di controllo dello Stato membro YY è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal titolare del trattamento CC, il cui stabilimento principale è in YY. L'autorità di controllo competente dello Stato membro XX informa l'autorità di controllo capofila (YY) di un reclamo proposto all'autorità di controllo XX che incide in modo sostanziale unicamente su interessati in XX, a norma dell'articolo 56, paragrafi 2 e 3, GDPR. L'autorità di controllo capofila decide di trattare il caso.

L'autorità di controllo XX decide di trasmettere all'autorità di controllo capofila un progetto di decisione in conformità dell'articolo 56, paragrafo 4, GDPR. L'autorità di controllo capofila predispone un progetto di decisione a norma dell'articolo 60, paragrafo 3, GDPR e lo trasmette all'autorità di controllo interessata. L'autorità di controllo XX ritiene che nel predisporre il progetto di decisione, l'autorità di controllo capofila sia venuta meno all'obbligo di tenere nella massima considerazione il progetto da lei trasmesso, a norma dell'articolo 56, paragrafo 4, GDPR, in quanto il progetto di decisione dell'autorità di controllo capofila non fornisce la motivazione del suo discostarsi dal progetto da lei trasmesso.

Di conseguenza, l'autorità di controllo XX solleva un'obiezione pertinente e motivata nella quale espone gli argomenti che specificano le diverse conclusioni a cui il progetto di decisione sarebbe giunto se l'autorità di controllo capofila si fosse conformata al suo progetto di decisione, in termini di accertamento della violazione o di determinazione delle azioni previste nei confronti del titolare del trattamento, allo scopo di evitare i rischi dimostrati per i diritti e le libertà fondamentali dell'interessato e, ove applicabile, per la libera circolazione dei dati personali all'interno dell'Unione.

31. Un'obiezione sollevata a norma dell'articolo 60, paragrafo 4, e dell'articolo 65, paragrafo 1, lettera a), GDPR lascia impregiudicata la disposizione di cui all'articolo 65, paragrafo 1, lettera b), GDPR. Pertanto un disaccordo in merito all'autorità cui spetta il ruolo di autorità di controllo capofila in un caso specifico non dovrebbe essere oggetto di un'obiezione ai sensi dell'articolo

60, paragrafo 4, GDPR ed esula dall'ambito di applicazione dell'articolo 4, punto 24, GDPR. L'EDPB ritiene che, a differenza di quanto accade per l'obiezione sollevata ai sensi dell'articolo 60, paragrafo 4, GDPR, la procedura in conformità dell'articolo 65, paragrafo 1, lettera b), GDPR sia applicabile in qualsiasi fase.

3.1.2 CONFORMITÀ AL GDPR DELL'AZIONE PREVISTA NEL PROGETTO DI DECISIONE IN RELAZIONE AL TITOLARE DEL TRATTAMENTO O AL RESPONSABILE DEL TRATTAMENTO

32. In questa seconda circostanza, il contenuto dell'obiezione pertinente e motivata consiste in un disaccordo in merito alla specifica misura correttiva proposta dall'autorità di controllo capofila o a un'altra azione prevista nel progetto di decisione.

33. Più nello specifico, l'obiezione pertinente e motivata dovrebbe chiarire i motivi per cui l'azione prevista nel progetto di decisione non sia conforme al GDPR. A questo scopo, l'autorità di controllo interessata deve esporre chiaramente gli elementi fattuali e/o gli argomenti giuridici alla base della diversa valutazione della situazione, indicando l'azione che l'autorità di controllo capofila dovrebbe adottare e includere nella decisione finale.

Esempio 5

Il titolare del trattamento ha comunicato dati medici sensibili del reclamante a terzi senza basarsi su un fondamento giuridico. Nel progetto di decisione, l'autorità di controllo capofila ha proposto di rivolgere un ammonimento. L'autorità di controllo interessata, invece, fornisce elementi fattuali a dimostrazione del fatto che il titolare del trattamento presenta problemi ampi e sistematici nel conformarsi al GDPR (ad esempio, trasmette regolarmente i dati dei propri clienti a terzi senza fondamento giuridico). Propone pertanto che sia ingiunto al titolare del trattamento di rendere conformi i trattamenti oppure che gli sia imposto un divieto provvisorio di trattamento dei dati o che gli sia inflitta una sanzione pecuniaria.

Esempio 6

A causa di un errore di uno dei suoi dipendenti, il titolare del trattamento ha pubblicato sul proprio sito web i nomi, i cognomi e i numeri di telefono di tutti i suoi 100 000 clienti. Questi dati personali sono stati accessibili al pubblico per due giorni. Considerato che il titolare del trattamento si è attivato il prima possibile, che l'errore è stato notificato e che tutti i clienti sono stati informati personalmente, l'autorità di controllo capofila ha previsto di rivolgere solo un ammonimento. Un'autorità di controllo interessata ritiene tuttavia che, trattandosi di una violazione dei dati su vasta scala che può avere ripercussioni o comportare un rischio per la vita privata dei clienti, sarebbe necessario infliggere una sanzione pecuniaria.

34. Come sancito nell'ultima frase dell'articolo 65, paragrafo 1, lettera a), GDPR, la decisione vincolante dell'EDPB riguarda tutte le questioni oggetto dell'obiezione, in particolare nel caso di una violazione. Il considerando 150, quinta frase, GDPR, afferma che il meccanismo di coerenza può essere utilizzato anche per favorire un'applicazione coerente delle sanzioni amministrative pecuniarie, pertanto è possibile che l'obiezione contesti gli elementi su cui si basa il calcolo dell'ammontare della sanzione. In tale ambito, se l'EDPB individua carenze nelle argomentazioni che hanno condotto all'imposizione della sanzione pecuniaria in questione, incaricherà l'autorità di controllo capofila di ricalcolare la sanzione pecuniaria e di porre rimedio alle carenze individuate. La valutazione dell'EDPB in questi casi dovrebbe basarsi su criteri condivisi derivanti dall'articolo 83, paragrafi 1 e 2, GDPR e dalle linee guida per il calcolo delle sanzioni pecuniarie.

Esempio 7

L'autorità di controllo interessata, tenendo conto dei fatti relativi al caso, ritiene che la sanzione pecuniaria prevista dall'autorità di controllo capofila nel progetto di decisione non sia effettiva, proporzionata e dissuasiva, come previsto all'articolo 83, paragrafo 1, GDPR.

3.2 RILEVANZA DEI RISCHI POSTI DAL PROGETTO DI DECISIONE RIGUARDO AI DIRITTI E ALLE LIBERTÀ FONDAMENTALI DEGLI INTERESSATI E, OVE APPLICABILE, ALLA LIBERA CIRCOLAZIONE DEI DATI PERSONALI ALL'INTERNO DELL'UNIONE

3.2.1 SIGNIFICATO DI "RILEVANZA DEI RISCHI"

35. È importante tenere presente che l'obiettivo del lavoro svolto dalle autorità di controllo è tutelare i diritti e le libertà fondamentali degli interessati e agevolare la libera circolazione dei dati personali all'interno dell'Unione (articolo 4, punto 24, articolo 51 e considerando 123 GDPR).

36. **L'obbligo di dimostrare la rilevanza dei rischi posti dal progetto di decisione (ad esempio, a causa delle misure previste oppure dell'assenza di misure correttive) riguardo ai diritti e alle libertà degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione spetta all'autorità di controllo interessata**. La possibilità per le autorità di controllo interessate di fornire tale dimostrazione dipenderà anche dal livello di dettaglio del progetto di decisione e dalle informazioni precedentemente comunicate dall'autorità di controllo capofila, come sottolineato al punto 8.

37. Il termine "rischio" è menzionato in varie sezioni del GDPR, e precedenti linee guida dell'EDPB[10] lo definiscono come "*uno scenario che descrive un evento e le sue conseguenze, stimati in termini di gravità e probabilità*". L'articolo 4, punto 24, GDPR fa riferimento alla necessità di dimostrare "la rilevanza" dei ri-

schi posti dal progetto di decisione, il che significa dimostrare le implicazioni che il progetto di decisione potrebbe avere sui valori tutelati. L'autorità di controllo interessata dovrà a tal fine presentare argomenti sufficienti per dimostrare chiaramente che tali rischi sono significativi e plausibili per i diritti e le libertà fondamentali degli interessati e, ove applicabile, per la libera circolazione dei dati all'interno dell'Unione. La dimostrazione della rilevanza dei rischi non può essere dedotta dagli argomenti giuridici e/o fattuali forniti dall'autorità di controllo interessata, ma deve essere individuata e formulata in modo esplicito nell'obiezione.

38. È opportuno sottolineare che mentre un'obiezione pertinente e motivata deve sempre dimostrare chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati (cfr. sezione 3.2.2 di seguito), la dimostrazione dei rischi posti alla libera circolazione dei dati personali all'interno dell'Unione europea è richiesta soltanto "ove applicabile" (cfr. la sezione seguente 3.2.3).

3.2.2 RISCHI PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI

39. La questione in esame riguarda l'impatto che il progetto di decisione, nel suo insieme, potrebbe avere sui diritti e sulle libertà fondamentali degli interessati. Ciò può riguardare le conclusioni dell'autorità di controllo capofila in merito alla sussistenza o meno di una violazione del GDPR da parte del titolare o del responsabile del trattamento e/o l'imposizione di misure correttive.

40. L'approccio alla valutazione del rischio posto dal progetto di decisione non coincide con quello adottato da un titolare del trattamento che svolge una valutazione d'impatto sulla protezione dei dati al fine di determinare il rischio di un trattamento futuro. L'oggetto della valutazione è completamente differente, si tratta cioè degli effetti prodotti dalle conclusioni dell'autorità capofila come esposte nel progetto di decisione in merito alla sussistenza o meno di una violazione. Le conclusioni dell'autorità di controllo capofila possono comportare l'adozione di determinate misure (le "misure previste"). Come detto, l'autorità di controllo interessata deve dimostrare i rischi facendo riferimento al progetto di decisione nel suo complesso.

41. Il considerando 129 GDPR chiarisce che "*[è] opportuno che i poteri delle autorità di controllo siano esercitati nel rispetto di garanzie procedurali adeguate previste dal diritto dell'Unione e degli Stati membri, in modo imparziale ed equo ed entro un termine ragionevole" e che "ogni misura dovrebbe essere appropriata, necessaria e proporzionata al fine di assicurare la conformità al presente regolamento, tenuto conto delle circostanze di ciascun singolo caso, rispettare il diritto di ogni persona di essere ascoltata prima che nei suoi confronti sia adottato un provvedimento individuale che le rechi pregiudizio ed evitare costi superflui ed eccessivi disagi per le persone interessate*".

42. Pertanto, la valutazione dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati può fondarsi, fra l'altro, sull'appropriatezza, la necessità e la proporzionalità delle misure previste (o non previste) sulla base delle conclusioni relative alla sussistenza o meno di

una violazione e alle eventuali azioni correttive messe in atto dal titolare o dal responsabile del trattamento.

43. I rischi in questione, inoltre, possono riferirsi all'impatto del progetto di decisione sui diritti e sulle libertà fondamentali degli interessati i cui dati personali sono oggetto di trattamento da parte del titolare o del responsabile del trattamento, ma anche all'impatto sui diritti e sulle libertà fondamentali degli interessati i cui dati personali potrebbero essere trattati in futuro, come pure alla possibile riduzione delle violazioni del GDPR in futuro, qualora ciò sia suffragato dai fatti del caso in esame.

Esempio 7

Il progetto di decisione dell'autorità di controllo capofila ha concluso che il principio di minimizzazione dei dati sancito dall'articolo 5, paragrafo 1, lettera c), GDPR non è stato violato dal titolare del trattamento. Nella sua obiezione l'autorità di controllo interessata adduce elementi fattuali e argomenti giuridici per dimostrare che l'attività di trattamento svolta dal titolare del trattamento ha in realtà prodotto la violazione dell'articolo 5, paragrafo 1, lettera c), GDPR e sostiene che sia opportuno rivolgere un ammonimento al titolare. Per dimostrare la rilevanza dei rischi per i diritti e le libertà fondamentali degli interessati, l'autorità di controllo interessata sostiene che un mancato ammonimento per la violazione di un principio fondamentale stabilirebbe un precedente rischioso, in quanto si ometterebbe di segnalare la necessità di apportare correttivi alle attività di trattamento dei dati del titolare e si metterebbero in pericolo gli interessati i cui dati personali sono e saranno trattati da tale titolare.

3.2.3 RISCHI PER LA LIBERA CIRCOLAZIONE DEI DATI PERSONALI ALL'INTERNO DELL'UNIONE

44. Se l'obiezione si riferisce anche a questi particolari rischi, l'autorità di controllo interessata dovrà chiarire perché la ritenga "applicabile". Inoltre, un'obiezione che dimostri i rischi posti alla libera circolazione dei dati personali, ma non anche ai diritti e alle libertà degli interessati, non sarà ritenuta conforme alla soglia fissata dall'articolo 4, punto 24, GDPR.

45. La necessità di evitare limitazioni o divieti alla libera circolazione dei dati personali per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali è esplicitamente richiamata nel GDPR[11], che intende introdurre norme armonizzate in materia di protezione dei dati nell'UE e consentire la libera circolazione dei dati personali all'interno dell'Unione, garantendo al tempo stesso un elevato livello di protezione dei diritti e delle libertà delle persone fisiche, in particolare il loro diritto alla protezione dei dati personali.

46. I rischi per la libera circolazione dei dati personali all'interno dell'Unione

possono derivare da qualsiasi misura, compresa la decisione di un'autorità di controllo nazionale, che introduca limitazioni ingiustificate alla conservazione dei dati (ad esempio, disposizioni che obblighino un titolare del trattamento a conservare determinate informazioni in uno specifico Stato membro) e/o alla libera circolazione dei dati personali tra gli Stati membri (ad esempio, mediante la sospensione della circolazione dei dati o l'imposizione di limitazioni provvisorie o definitive, incluso il divieto di trattamento).

47. Allo stesso modo, la libera circolazione dei dati personali all'interno dell'Unione può essere messa a rischio qualora vengano definite aspettative (o imposti obblighi) sulle modalità di rispetto del GDPR da parte dei titolari del trattamento, segnatamente stabilendo un legame fra le azioni attese dai titolari del trattamento e una regione specifica dell'UE (ad esempio, mediante la previsione di specifici requisiti soggettivi).

48. Inoltre, la libera circolazione dei dati personali all'interno dell'Unione può essere ostacolata anche da decisioni ingiustificatamente diverse emesse dalle autorità di controllo in situazioni identiche o simili (ad esempio, in termini di settore o di tipo di trattamento), in quanto una tale difformità può mettere a repentaglio la parità di condizioni nell'UE, creare situazioni contraddittorie all'interno dell'Unione e condurre a una ricerca opportunistica del foro più vantaggioso. A tale riguardo, è opportuno tenere conto delle specificità nazionali ammesse dal GDPR per quanto concerne determinati settori, quali l'assistenza sanitaria, il giornalismo o gli archivi.

NOTE

[1] Nel presente documento con il termine "Stati membri" si intendono gli "Stati membri del SEE".

[2] Articolo 60, paragrafo 1, del regolamento (UE) 2016/679.

[3] Le autorità di controllo interessate possono ritirare le obiezioni precedentemente sollevate.

[4] Articolo 60, paragrafo 1, GDPR.

[5] Cfr. la formulazione dell'articolo 60, paragrafo 4, GDPR.

[6] A norma dell'articolo 60, paragrafo 4, GDPR, l'autorità di controllo capofila sottopone la questione al meccanismo di coerenza di cui all'articolo 63 anche ove non dia seguito all'obiezione pertinente e motivata.

[7] Cfr. il regolamento interno dell'EDPB.

[8] L'Oxford English Dictionary definisce il termine "relevant" ("pertinente") come "bearing on or connected with the matter in hand; closely relating to the subject or point at issue; pertinent to a specified thing" [in relazione o collegato con la materia in questione; che riguarda strettamente l'argomento o il punto in questione; pertinente a un determinato oggetto]; ("relevant, adj." OED Online, Oxford University Press, giugno 2020, www.oed.com/view/Entry/161893. Consultato il 24 luglio 2020).

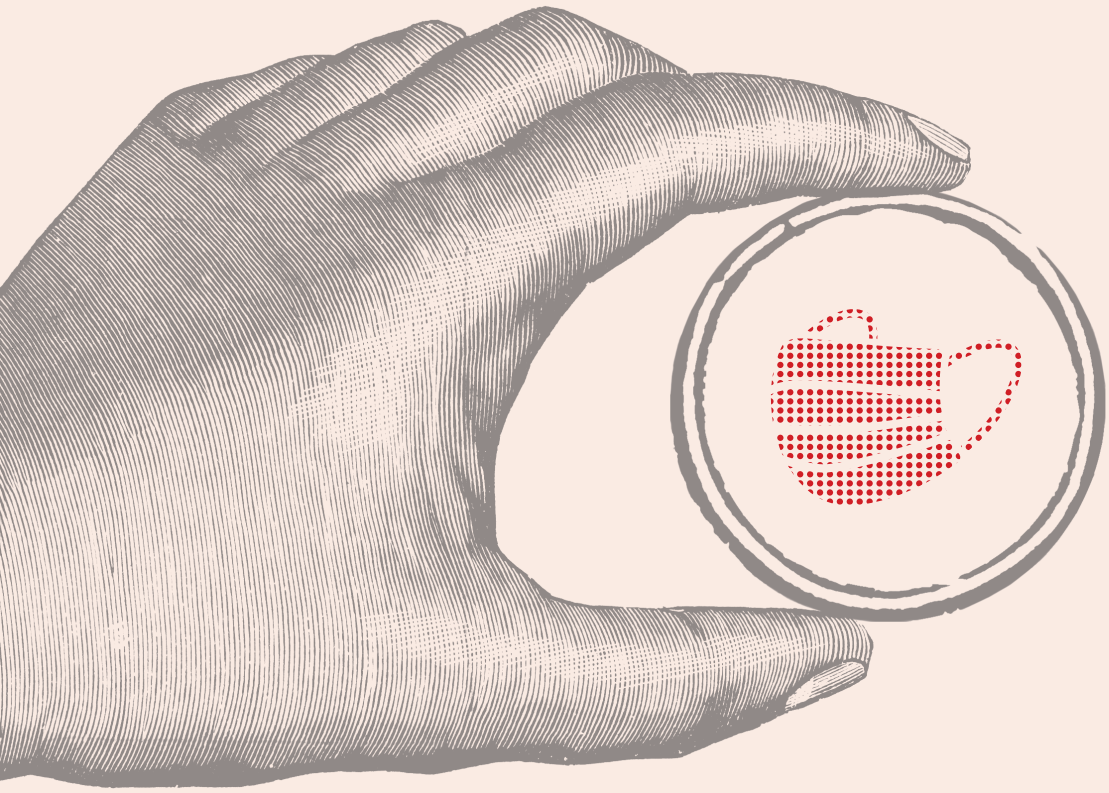
[9] L'Oxford English Dictionary definisce il termine "reasoned" ("motivato") come "characterised by or based on reasoning; carefully studied" [caratterizzato da o fondato su una motivazione; attentamente esaminato] ("reasoned, adj.2." OED Online, Oxford University Press, giugno 2020, www.oed.com/view/Entry/159078. Consultato il 24 luglio 2020).

[10] Cfr. ad esempio, le linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento 2016/679, WP 248 rev.01.

[11] Articolo 1, paragrafo 3, GDPR.

Torna a **Indice**

5 Covid - 19



Premessa Covid-19

La pandemia da Covid-19 e le strategie messe in atto per contrastarla a partire dal 2020, con le numerose ed evidenti implicazioni legate alla necessità di trattare ingenti quantità di dati personali di grande delicatezza, per finalità tanto di cura quanto di ricerca, hanno ovviamente sollecitato più volte i Garanti europei a porre in essere interventi chiarificatori e di indirizzo per i titolari pubblici e privati, sempre nello spirito di un approccio coordinato e coerente secondo i principi del regolamento europeo.

Il Comitato ha adottato una prima **dichiarazione** (19 marzo 2020) con la quale, muovendo dalla premessa che le norme di protezione dei dati non mettono a rischio le misure volte a contenere la pandemia, ha richiamato l'attenzione sulla necessità di garantire in ogni caso la liceità dei trattamenti dei dati effettuati e sul fatto che qualunque misura, anche restrittiva delle libertà, adottata in un contesto eccezionale come quello legato alla pandemia debba essere proporzionata e limitata al periodo dell'emergenza.

Una visione più generale e sistemica delle implicazioni legate al trattamento di dati relativi alla salute per fini di ricerca scientifica, nel contesto dell'emergenza da Covid-19, è stata poi sviluppata nelle **linee guida 3/2020**, che guardano all'impegno della comunità scientifica internazionale nella ricerca di rimedi efficaci e sicuri contro il virus. Le linee guida considerano in particolare la base giuridica del trattamento, la necessità di assicurare garanzie adeguate per tale trattamento e l'esercizio dei diritti dell'interessato, e ricordano che il GDPR prevede norme speciali per il trattamento dei dati relativi alla salute a fini di ricerca scientifica, applicabili anche nel contesto della pandemia da Covid-19, e che il legislatore nazionale di ciascuno Stato membro ha il potere di emanare norme specifiche ai sensi del GDPR (nel rispetto dei principi dell'art. 5 del GDPR e della giurisprudenza della CGUE) al fine di consentire tali trattamenti. Le deroghe e le limitazioni relative alla protezione dei dati consentite dal GDPR devono pertanto applicarsi solo nella misura strettamente necessaria al perseguimento dello

scopo, e si richiama la necessità di valutare con attenzione se debba essere effettuata una valutazione d'impatto sulla protezione dei dati nei singoli casi individuando periodi di conservazione proporzionati in rapporto alla durata e allo scopo della ricerca.

Anche le **linee guida 4/2020** affrontano un aspetto importante legato all'emergenza da Covid-19, ossia le condizioni e i principi da rispettare ai fini di un impiego proporzionato degli strumenti che utilizzano i dati di localizzazione e il tracciamento dei contatti. Le linee guida prendono in esame due ambiti specifici: a) l'utilizzo dei dati di localizzazione a supporto della risposta alla pandemia tramite la definizione di modelli della diffusione del virus; b) l'impiego del tracciamento dei contatti per informare le persone potenzialmente entrate in contatto ravvicinato con soggetti successivamente confermati positivi. Le linee guida sottolineano che tanto il GDPR quanto la direttiva e-privacy contengono specifiche disposizioni sull'utilizzo di dati anonimi o personali a supporto delle autorità pubbliche e di altri soggetti, a livello nazionale ed europeo, nelle attività di monitoraggio e contenimento della diffusione del Covid-19. Tutte le misure adottate dagli Stati membri o dall'UE che comportino il trattamento di dati personali per il contrasto del Covid-19 devono essere conformi ai principi generali di efficacia, necessità e proporzionalità. Un punto essenziale per i Garanti europei è che l'impiego di app per il tracciamento dei contatti avvenga su base volontaria senza comportare il tracciamento degli spostamenti individuali, facendo invece perno sulle informazioni di prossimità relative agli utenti. Da segnalare anche la pubblicazione di una "guida" per le app di tracciamento dei contatti, allegata al documento, che intende fornire indicazioni generali ai progettisti e agli sviluppatori delle app di tracciamento.

Linee guida 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19

Adottate il 21 aprile 2020

Cronologia delle versioni

Versione 1.1	30 aprile	Piccole correzioni
Versione 1.0	21 aprile 2020	Adozione delle Linee guida

Indice

1 Introduzione

2 Applicazione del regolamento generale sulla protezione dei dati

3 Definizioni
- 3.1 “Dati relativi alla salute”
- 3.2 “Trattamento a fini di ricerca scientifica”
- 3.3 “Trattamento ulteriore”

4 Base giuridica del trattamento
- 4.1 Consenso
- 4.2 Legislazioni nazionali

5 Principi relativi alla protezione dei dati
- 5.1 Trasparenza e informazione degli interessati
  - 5.1.1 Quando deve essere informato l’interessato?
  - 5.1.2 Esenzioni
- 5.2 Limitazione della finalità e presunzione di compatibilità
- 5.3 Minimizzazione dei dati e conservazione limitata
- 5.4 Integrità e riservatezza

6 Esercizio dei diritti dell’interessato

7 Trasferimenti internazionali di dati per scopi di ricerca scientifica

8 Sintesi

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

Visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in prosieguo "RGPD"),

Visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificato dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018,

Visti l'articolo 12 e l'articolo 22 del suo regolamento,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

1. INTRODUZIONE

1. A causa della pandemia causata dal COVID-19, attualmente sono in corso grandi sforzi di ricerca scientifica nella lotta contro il SARS-CoV-2 al fine di giungere a risultati quanto più rapidamente possibile.
2. Nel contempo, continuano a porsi questioni giuridiche riguardanti l'uso di dati relativi alla salute ai sensi dell'articolo 4, paragrafo 15, del regolamento generale sulla protezione dei dati per fini di ricerca. Le presenti linee guida mirano a far luce sulle questioni più urgenti, quali la base giuridica del trattamento, la messa in atto di garanzie adeguate per tale trattamento e l'esercizio dei diritti dell'interessato.
3. Si ricorda che lo sviluppo di ulteriori e più dettagliati orientamenti per il trattamento dei dati relativi alla salute ai fini della ricerca scientifica fa parte del piano di lavoro annuale del comitato europeo per la protezione dei dati. Si noti, inoltre, che le presenti linee guida non prendono in esame il trattamento dei dati personali per scopi di sorveglianza epidemiologica.

2. APPLICAZIONE DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

4. Le norme in materia di protezione dei dati (come il Regolamento generale sulla protezione dei dati, RGPD) non ostacolano le misure adottate nella lotta contro la pandemia da COVID-19.[1] Il RGPD è un testo legislativo di ampio respiro e contiene varie disposizioni che consentono di trattare i dati personali per finalità di ricerca scientifica connesse alla pandemia da COVID-19 nel rispetto dei diritti fondamentali alla vita privata e alla protezione dei dati personali.[2] Il RGPD prevede anche una deroga specifica al divieto di trattamento di talune categorie particolari di dati personali, come i dati relativi alla salute, qualora ciò sia necessario per tali finalità di ricerca scientifica. [3]
5. Nel trattamento di dati relativi alla salute per scopi scientifici connessi alla pandemia da COVID-19 devono trovare applicazione i diritti fondamentali riconosciuti nell'UE. Le norme sulla protezione dei dati non prevalgono sulla libertà di scienza sancita dall'articolo 13 della Carta dei diritti fondamentali dell'UE, né questa su quelle. Piuttosto, sono necessari una valutazione e un bilanciamento attenti di questi diritti e libertà, che deve tradursi in un risultato rispettoso dell'essenza di entrambe le componenti.

3. DEFINIZIONI

6. È importante comprendere quali operazioni di trattamento possano beneficiare del regime speciale previsto nel RGPD e oggetto degli approfondimenti qui svolti. Pertanto, occorre definire i termini "dati relativi alla salute", "trattamento a fini di ricerca scientifica" e "trattamento ulteriore" (rispetto a quest'ultima definizione, si parla anche di "utilizzo primario e secondario dei dati sanitari").

3.1 "DATI RELATIVI ALLA SALUTE"

7. Ai sensi dell'articolo 4, paragrafo 15, del RGPD, per "*dati relativi alla salute*" si intendono i dati personali relativi alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni circa il suo stato di salute. Come indicato nel considerando 53, i dati relativi alla salute meritano una protezione più elevata, in quanto l'uso di tali dati sensibili può avere gravi ripercussioni negative per gli interessati. Alla luce di ciò e della pertinente giurisprudenza della Corte di giustizia dell'Unione europea ("CGUE"),[4] l'espressione "dati relativi alla salute" deve essere interpretata in modo estensivo.
8. I dati relativi alla salute possono essere ricavati da fonti diverse, quali per esempio:
    1. Informazioni raccolte da un fornitore di assistenza sanitaria in una cartella clinica (anamnesi e risultati di esami e trattamenti).
    2. Informazioni che diventano dati relativi alla salute sulla base di riferimenti incrociati ad altri dati tali da rivelare lo stato di salute o i rischi per la salute (ad esempio, la presunzione che una determinata persona sia esposta a un rischio più elevato di attacchi cardiaci basata su misurazioni ripetute della pressione arteriosa lungo un certo arco di tempo).
    3. Informazioni ricavate da test di autovalutazione, in cui gli interessati rispondono a domande relative alla loro salute (ad esempio, descrivendo sintomatologia).
    4. Informazioni che diventano dati relativi alla salute a seguito del loro utilizzo in un contesto specifico (ad esempio, informazioni relative a un viaggio recente o alla permanenza in una regione interessata dal COVID-19 elaborate da un professionista sanitario per effettuare una diagnosi).

3.2 "TRATTAMENTO A FINI DI RICERCA SCIENTIFICA"

9. L'articolo 4 del RGPD non prevede una definizione esplicita di "trattamento a fini di ricerca scientifica". Come indicato nel considerando 159, "*il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato e includere ad esempio sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati, oltre a tenere conto dell'obiettivo dell'Unione di istituire uno spazio europeo della ricerca ai sensi dell'articolo 179, paragrafo 1, TFUE. Le finalità di ricerca scientifica dovrebbero altresì includere gli studi svolti nell'interesse pubblico nel settore della sanità pubblica*".
10. Tuttavia, il Gruppo di lavoro « Articolo 29 » ha già sottolineato che il termine non può essere interpretato estensivamente travalicandone il significato comune, e in questo contesto intende per "ricerca scientifica" "*un progetto di ricerca istituito conformemente alle pertinenti norme etiche e metodologiche settoriali, in conformità delle buone prassi*".[5]

3.3 “TRATTAMENTO ULTERIORE”

11. Infine, rispetto al “trattamento di dati sanitari a fini di ricerca scientifica” occorre distinguere fra due tipologie di dati:
    1. Ricerca su dati personali (relativi alla salute) consistente nell’impiego di dati raccolti direttamente per scopi di studio scientifico (“utilizzo primario”).
    2. Ricerca su dati personali (relativi alla salute) consistente nel trattamento ulteriore di dati inizialmente raccolti per altre finalità (“utilizzo secondario”).
12. **Esempio 1**: Per condurre una sperimentazione clinica su persone con sospetta infezione da SARS-CoV-2, vengono raccolti dati relativi alla salute e si utilizza un questionario. Si tratta di un caso di “utilizzo primario” dei dati relativi alla salute come sopra definiti.
13. **Esempio 2**: L’interessato, in qualità di paziente, ha consultato un operatore sanitario riguardo a sintomi da SARS-CoV-2. Se i dati relativi alla salute registrati dall’operatore sanitario vengono successivamente utilizzati a fini di ricerca scientifica, tale utilizzo è classificato come un trattamento ulteriore dei dati relativi alla salute (utilizzo secondario) raccolti inizialmente per un diverso scopo.
14. La distinzione tra ricerca scientifica basata sull’utilizzo primario o secondario dei dati relativi alla salute assume particolare importanza al fine di determinare la base giuridica del trattamento, gli obblighi di informazione e l’applicazione del principio della limitazione delle finalità a norma dell’articolo 5, paragrafo 1, lettera b), del RGPD, come illustrato di seguito.

4. BASE GIURIDICA DEL TRATTAMENTO

15. Tutti i trattamenti di dati personali relativi alla salute devono essere conformi ai principi in materia di trattamento di cui all’articolo 5 del RGPD e a uno dei fondamenti di liceità e alle deroghe specifiche indicati rispettivamente all’articolo 6 e all’articolo 9 del RGPD affinché sia assicurata la liceità del trattamento di tale categoria particolare di dati personali.[6]
16. Le basi giuridiche e le deroghe applicabili per il trattamento dei dati relativi alla salute a fini di ricerca scientifica sono previste rispettivamente all’articolo 6 e all’articolo 9. Nella sezione seguente sono esaminate le norme relative al consenso e alla legislazione nazionale pertinente. Va osservato che non esiste una gerarchia tra le basi giuridiche stabilite nel RGPD.

4.1 CONSENSO

17. Il consenso dell’interessato, raccolto a norma dell’articolo 6, paragrafo 1, lettera a), e dell’articolo 9, paragrafo 2, lettera a), del regolamento generale sulla protezione dei dati, può costituire la base giuridica per il trattamento dei dati relativi alla salute nel contesto del COVID-19.

18. Va tuttavia osservato che devono essere soddisfatte tutte le condizioni previste ai fini di un consenso esplicito, in particolare quelle di cui all'articolo 4, paragrafo 11, all'articolo 6, paragrafo 1, lettera a), all'articolo 7 e all'articolo 9, paragrafo 2, lettera a), del regolamento generale sulla protezione dei dati. In particolare, il consenso deve essere libero, specifico, informato e inequivocabile e deve essere prestato mediante dichiarazione o "azione positiva inequivocabile".

19. Come indicato al considerando 43, il consenso non può essere considerato libero se vi è un evidente squilibrio tra l'interessato e il titolare del trattamento. È quindi importante che un interessato non sia sottoposto a pressioni e non sia penalizzato se decide di non dare il proprio consenso. Il Comitato ha già esaminato la tematica del consenso nel contesto delle sperimentazioni cliniche.[7] Ulteriori orientamenti, in particolare per quanto riguarda il requisito del consenso esplicito, sono reperibili nelle Linee guida in materia di consenso del Gruppo di lavoro « Articolo 29 ».[8]

20. **Esempio**: Viene condotta un'indagine nell'ambito di uno studio osservazionale su una determinata popolazione, riguardante la sintomatologia e l'evoluzione di una patologia. Per il trattamento di tali dati relativi alla salute, i ricercatori possono chiedere il consenso dell'interessato alle condizioni stabilite dall'articolo 7 del RGPD.

21. A giudizio del Comitato, l'esempio di cui sopra non configura un "evidente squilibrio", come indicato al considerando 43, e l'interessato dovrebbe essere in grado di dare il consenso ai ricercatori.[9] Nell'esempio, gli interessati non versano in alcun modo in una situazione di dipendenza dai ricercatori tale da influenzare in modo improprio l'esercizio della loro libera volontà; è altresì chiaro che non subiranno conseguenze negative se rifiutano di dare il loro consenso.

22. Tuttavia, i ricercatori dovrebbero essere consapevoli del fatto che, se si utilizza il consenso come base legale per il trattamento, l'interessato deve avere la possibilità di revocare tale consenso in qualsiasi momento, ai sensi dell'articolo 7, paragrafo 3, del RGPD. In caso di revoca del consenso, tutti i trattamenti che si fondavano sul consenso restano legittimi, conformemente al RGPD, ma il titolare deve cessare le attività di trattamento in questione e, in assenza di altra base giuridica che giustifichi la conservazione a fini di ulteriore trattamento, i dati dovrebbero essere cancellati.[10]

4.2 LEGISLAZIONI NAZIONALI

23. L'articolo 6, paragrafo 1, lettera e), o lettera f), del RGPD, in combinato disposto con le deroghe di cui all'articolo 9, paragrafo 2, lettera j), o lettera i), del RGPD, possono fornire una base giuridica per il trattamento dei dati personali (relativi alla salute) a fini di ricerca scientifica. Il Comitato ha già fornito chiarimenti in merito nel contesto dei trattamenti per finalità di sperimentazione clinica.[11]

24. **Esempio**: Uno studio su larga scala relativo a una popolazione di pazienti COVID-19 che utilizzi le rispettive cartelle cliniche.

25. Come indicato in precedenza, l'UE e il legislatore nazionale di ciascuno Stato membro possono emanare norme specifiche a norma dell'articolo 9, paragrafo 2, lettera j), o dell'articolo 9, paragrafo 2, lettera i), del RGPD allo scopo di fornire una base giuridica per il trattamento dei dati relativi alla salute a fini di ricerca scientifica. Pertanto, le condizioni e la portata di tale trattamento variano a seconda del diritto nazionale del singolo Stato membro.

26. Ai sensi dell'articolo 9, paragrafo 2, lettera i), del RGPD, il diritto in questione deve prevedere "misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale". Come prevede in modo analogo l'articolo 9, paragrafo 2, lettera j), del RGPD, le norme di diritto in questione devono « essere proporzionate allo scopo perseguito, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell' interessato".

27. Inoltre, tali norme di diritto devono essere interpretate alla luce dei principi di cui all'articolo 5 del RGPD e della giurisprudenza della Corte di giustizia. In particolare, le deroghe e le limitazioni relative alla protezione dei dati di cui all'articolo 9, paragrafo 2, lettera j), e all'articolo 89 del RGPD devono applicarsi solo nella misura strettamente necessaria.[12]

5. PRINCIPI RELATIVI ALLA PROTEZIONE DEI DATI

28. Titolari e responsabili del trattamento devono rispettare i principi relativi al trattamento dei dati personali fissati nell'articolo 5 del RGPD, in particolare considerando i grandi volumi di dati personali che possono essere trattati a fini di ricerca scientifica. Nel contesto delle presenti Linee guida i paragrafi seguenti affrontano gli aspetti più importanti dei principi in questione.

5.2 TRASPARENZA E INFORMAZIONE DEGLI INTERESSATI

29. Il principio di trasparenza impone che i dati personali siano trattati in modo corretto e trasparente nei confronti dell'interessato. Tale principio è strettamente connesso agli obblighi di informazione ai sensi dell'articolo 13 o dell'articolo 14 del RGPD.

30. In via generale, l'interessato deve essere informato individualmente dell'esistenza del trattamento e del fatto che suoi dati personali (relativi alla salute) sono trattati a fini scientifici. Le informazioni fornite dovrebbero contenere tutti gli elementi di cui all'articolo 13 o all'articolo 14 del RGPD.

31. Occorre notare che i ricercatori trattano spesso dati relativi alla salute che non hanno ottenuto direttamente dall'interessato, ad esempio perché utilizzano dati provenienti da cartelle cliniche o relativi a pazienti di altri paesi.

Pertanto, la presente sezione sarà incentrata sull'articolo 14 del RGPD, che disciplina gli obblighi in materia di informazione qualora i dati personali non siano raccolti direttamente presso l'interessato.

5.1.1 QUANDO DEVE ESSERE INFORMATO L'INTERESSATO?

32. Qualora i dati personali non siano stati ottenuti presso l'interessato, l'articolo 14, paragrafo 3, lettera a), del RGPD prevede che il titolare lo informi "entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati".

33. Nel contesto che ci interessa, va osservato in particolare che, a norma dell'articolo 14, paragrafo 4, del RGPD, qualora "il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità".

34. In caso di trattamento ulteriore dei dati a fini scientifici, e tenendo conto della sensibilità dei dati in questione, una tutela adeguata ai sensi dell'articolo 89, paragrafo 1, consiste nel fornire all'interessato le informazioni entro un periodo di tempo ragionevole prima dell'attuazione del nuovo progetto di ricerca. Ciò consente all'interessato di venire a conoscenza del progetto di ricerca e di esercitare preventivamente i suoi diritti.

5.1.2 ESENZIONI

35. Tuttavia, l'articolo 14, paragrafo 5), del RGPD prevede quattro esenzioni dall'obbligo di informazione. Nel contesto che qui ci interessa, risultano particolarmente pertinenti l'esenzione ai sensi dell'articolo 14, paragrafo 5, lettera (b) ("risulta impossibile o implicherebbe uno sforzo sproporzionato") e (c) ("l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro »), in particolare per quanto riguarda gli obblighi di informazione di cui all'articolo 14, paragrafo 4, del RGPD.

5.1.2.1 Risulta impossibile

36. Nelle Linee guida relative al principio di trasparenza,[13] il Gruppo di lavoro « Articolo 29 » ha già sottolineato che "La situazione in cui la comunicazione delle informazioni "risulta impossibile" ai sensi dell'articolo 14, paragrafo 5, lettera b), è del tipo "bianco o nero", perché una certa cosa è impossibile oppure non lo è: non esistono gradazioni di impossibilità. Pertanto, se intende valersi dell'eccezione, il titolare del trattamento deve dimostrare i fattori che effettivamente gli impediscono di fornire le informazioni all'interessato. Se, trascorso un certo periodo di tempo, i fattori che hanno determinato l'"impossibilità" svaniscono e la comunicazione delle informazioni all'interessa-

to diventa possibile, il titolare del trattamento dovrebbe provvedervi immediatamente. In pratica, vi saranno pochissime situazioni in cui il titolare del trattamento potrà dimostrare l'effettiva impossibilità di fornire le informazioni all'interessato; (...)".

5.1.2.2 Sforzo sproporzionato

37. Nel definire che cosa debba intendersi per sforzo sproporzionato, il considerando 62 fa riferimento al numero di interessati, all'antichità dei dati e alla sussistenza di garanzie adeguate quali possibili indicatori. Nelle Linee guida in materia di trasparenza di cui sopra,[14] si raccomanda al titolare del trattamento di effettuare un bilanciamento al fine di valutare lo sforzo richiesto per fornire le informazioni tenendo conto dell'impatto e degli effetti sull'interessato qualora quest'ultimo non sia in possesso delle informazioni specifiche.
38. Esempio: L'esistenza di un numero considerevole di interessati per i quali non si dispone di informazioni di contatto potrebbe configurare uno sforzo sproporzionato rispetto alla prestazione delle informative.

5.1.2.3 Grave pregiudizio al conseguimento degli obiettivi

39. Per potersi avvalere di tale eccezione, i titolari del trattamento devono dimostrare che la comunicazione delle informazioni di cui all'articolo 14, paragrafo 1, di per sé rende impossibile o pregiudica gravemente il conseguimento degli obiettivi del trattamento.
40. Qualora si applichi l'eccezione di cui all'articolo 14, paragrafo 5, lettera b), del RGPD, "il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni".

5.1.2.4 L'ottenimento o la comunicazione dei dati sono espressamente previsti dal diritto dell'Unione o dello Stato membro

41. L'articolo 14, paragrafo 5, lettera c), del RGPD consente una deroga alle prescrizioni in materia di informazione di cui all'articolo 14, paragrafi (1), (2) e (4), nella misura in cui l'ottenimento o la comunicazione di dati personali "sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento". Tale deroga è subordinata alla condizione che il diritto in questione preveda "misure appropriate per tutelare i legittimi interessi dell'interessato". Come indicato nelle Linee guida sulla trasparenza di cui sopra,[15] la norma di diritto in questione deve indirizzarsi direttamente al titolare del trattamento e prevedere un obbligo di ottenimento o comunicazione specificamente riferito al titolare. Per fare affidamento su tale esenzione, il Comitato ricorda che il titolare deve essere in grado di dimostrare in che modo la norma in questione gli si applichi direttamente e gli imponga di ottenere o comunicare i dati personali.

5.2 LIMITAZIONE DELLA FINALITÀ E PRESUNZIONE DI COMPATIBILITÀ

42. Di norma, i dati sono "raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità" ai sensi dell'articolo 5, paragrafo 1, lettera b), del RGPD.

43. Tuttavia, la "presunzione di compatibilità" di cui all'articolo 5, paragrafo 1, lettera b), del RGPD stabilisce che "un ulteriore trattamento [...] per finalità [...] di ricerca scientifica [...] non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali". Questa tematica, a causa della sua natura orizzontale e complessa, sarà esaminata in maggiore dettaglio nelle linee guida di prossima pubblicazione da parte del Comitato sul trattamento dei dati relativi alla salute a fini di ricerca scientifica.

44. L'articolo 89, paragrafo 1, del RGPD stabilisce che il trattamento dei dati a fini di ricerca "è soggetto a garanzie adeguate" tali da « garantire che siano in atto misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio di minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo".

45. I requisiti di cui all'articolo 89, paragrafo 1, del RGPD evidenziano l'importanza del principio di minimizzazione e dei principi di integrità e riservatezza nonché del principio della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita (cfr. infra).[16] Di conseguenza, tenuto conto della natura sensibile dei dati relativi alla salute e dei rischi connessi al riutilizzo di tali dati a fini di ricerca scientifica, devono essere adottate misure robuste al fine di garantire un adeguato livello di sicurezza, come richiesto dall'articolo 32, paragrafo 1, del RGPD.

5.3 MINIMIZZAZIONE DEI DATI E CONSERVAZIONE LIMITATA

46. Nell'ambito della ricerca scientifica, è possibile rispettare il principio di minimizzazione prevedendo l'obbligo di specificare i quesiti di ricerca e di valutare la tipologia e la quantità di informazioni necessarie per rispondere adeguatamente a tali quesiti. La definizione dei dati necessari dipenderà sempre dalla finalità della ricerca, anche quando quest'ultima ha natura esplorativa, e dovrebbe avvenire nel rispetto del principio della limitazione delle finalità a norma dell'articolo 5, paragrafo 1, lettera b), del RGPD. Va osservato che i dati devono essere resi anonimi quando è possibile effettuare una ricerca scientifica con dati anonimizzati.

47. Inoltre, devono essere fissati periodi di conservazione proporzionati. Come previsto dall'articolo 5, paragrafo 1, lettera e), del RGPD, "i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse [...] di ricerca scientifica [...] conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato".

48. Nel definire i periodi di conservazione, dovrebbero essere tenuti in considerazione criteri quali la durata e lo scopo della ricerca. Occorre osservare che disposizioni nazionali possono disciplinare il periodo di conservazione.

5.4 INTEGRITÀ E RISERVATEZZA

49. Come indicato in precedenza, informazioni sensibili quali i dati relativi alla salute meritano maggiore protezione in quanto il loro trattamento si associa a una maggiore probabilità di impatti negativi per gli interessati. Ciò vale in modo particolare nel contesto dell'epidemia di COVID-19, poiché il prevedibile riutilizzo dei dati relativi alla salute a fini scientifici accresce la numerosità e l'eterogeneità dei soggetti che possono trattare tali dati.
50. Va osservato che il principio di integrità e riservatezza deve essere letto in combinato disposto con i requisiti di cui all'articolo 32, paragrafo 1, e all'articolo 89, paragrafo 1, del RGPD. Le disposizioni citate devono essere rispettate integralmente. Pertanto, tenuto conto dei rischi elevati di cui sopra, occorre implementare misure tecniche e organizzative adeguate per garantire un livello sufficiente di sicurezza.
51. Tali misure dovrebbero prevedere almeno il ricorso alla pseudonimizzazione,[17] alla cifratura, ad accordi di non divulgazione e rigide disposizioni in materia di autorizzazioni, restrizioni e registrazioni degli accessi ai dati. Va osservato che le disposizioni nazionali possono prevedere requisiti tecnici specifici o altre garanzie quali il rispetto delle norme in materia di segreto professionale.
52. Inoltre, dovrà essere effettuata una valutazione d'impatto sulla protezione dei dati conformemente all'articolo 35 del RGPD quando il trattamento "*può comportare un rischio elevato per i diritti e le libertà delle persone fisiche*" ai sensi dell'articolo 35, paragrafo 1, del RGPD. Si tiene conto, al riguardo, degli elenchi di cui all'articolo 35, paragrafi 4 e 5, del RGPD.
53. Il Comitato sottolinea l'importanza dei responsabili della protezione dei dati. Se del caso, dovrebbero essere consultati i responsabili della protezione dei dati in merito al trattamento dei dati relativi alla salute per scopi di ricerca scientifica nel contesto dell'emergenza causata dal COVID-19.
54. Infine, le misure adottate per proteggere i dati (anche durante i trasferimenti) dovrebbero essere adeguatamente documentate nel registro delle attività di trattamento.

6. ESERCIZIO DEI DIRITTI DELL'INTERESSATO

55. In linea di principio, situazioni quali l'attuale emergenza dovuta al COVID-19 non sospendono né limitano la possibilità degli interessati di esercitare i loro diritti ai sensi degli articoli 12-22 del RGPD. Tuttavia, l'articolo 89, paragrafo 2, del RGPD consente al legislatore nazionale di limitare (in alcuni casi) i diritti dell'interessato di cui al capo 3 del regolamento. Di conseguen-

za, possono aversi *differenti* limitazioni dei diritti degli interessati a seconda del diritto del singolo Stato membro.

56. Inoltre, alcune limitazioni dei diritti degli interessati trovano fondamento direttamente nelle disposizioni del regolamento, come le restrizioni relative all'accesso ai sensi dell'articolo 15, paragrafo 4, del RGPD e la limitazione del diritto alla cancellazione a norma dell'articolo 17, paragrafo 3, lettera d), del RGPD. Si è già detto delle esenzioni dall'obbligo di informazione a norma dell'articolo 14, paragrafo 5, del RGPD.

57. Va osservato che, alla luce della giurisprudenza della Corte di giustizia europea, ogni limitazione dei diritti degli interessati deve applicarsi solo nella misura strettamente necessaria.[18]

7. TRASFERIMENTI INTERNAZIONALI DI DATI PER SCOPI DI RICERCA SCIENTIFICA

58. Nel contesto della ricerca, e in particolare nel contesto della pandemia da COVID-19, sarà probabilmente necessaria una cooperazione internazionale che potrebbe comportare trasferimenti internazionali di dati relativi alla salute per finalità di ricerca scientifica al di fuori del SEE.

59. Quando i dati personali sono trasferiti verso un paese non appartenente al SEE o verso un'organizzazione internazionale, oltre a rispettare le norme stabilite nel RGPD,[19] in particolare l'articolo 5 (principi di protezione dei dati), l'articolo 6 (liceità) e l'articolo 9 (categorie particolari di dati[20]), l'esportatore deve conformarsi anche alle previsioni del Capo V (trasferimenti di dati).[21]

60. In aggiunta al generale obbligo di trasparenza di cui alla pagina 7 delle presenti Linee guida, l'esportatore dei dati è tenuto a informare gli interessati dell'intenzione di trasferire dati personali verso un paese terzo o un'organizzazione internazionale. Ciò comprende informazioni sull'esistenza o sull'assenza di una decisione di adeguatezza da parte della Commissione europea o sul fatto che il trasferimento sia basato su una delle garanzie adeguate di cui all'articolo 46, ovvero su una delle deroghe di cui all'articolo 49, paragrafo 1. Tale obbligo sussiste indipendentemente dal fatto che i dati personali siano stati ottenuti direttamente dall'interessato o meno.

61. In linea generale, nel valutare come gestire tali condizioni applicabili al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, è opportuno che gli esportatori di dati valutino i rischi per i diritti e le libertà degli interessati connessi a ciascun trasferimento[22], privilegiando soluzioni che garantiscano agli interessati la tutela ininterrotta dei diritti fondamentali e delle garanzie di cui godono con riguardo al trattamento dei loro dati, anche una volta che questi siano stati trasferiti. È questo il caso dei trasferimenti verso paesi che dispongono di un livello adeguato di protezione[23], oppure qualora si utilizzi una delle garanzie adeguate di cui all'articolo 46 del RGPD[24] cui si associa la disponibilità per gli interessati di diritti azionabili e mezzi di ricorso efficaci.

62. In assenza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, del RGPD o di garanzie adeguate ai sensi dell'articolo 46 di quest'ultimo, l'articolo 49 del RGPD prevede alcune situazioni specifiche in cui il trasferimento di dati personali può avvenire in via eccezionale. Le deroghe previste dall'articolo 49 del regolamento sono, pertanto, eccezioni alla regola generale e devono essere interpretate in modo restrittivo e caso per caso.[25] Con riguardo all'attuale crisi dovuta al COVID-19, possono trovare applicazione le deroghe di cui all'articolo 49, paragrafo 1, lettera d) ("trasferimento necessario per importanti motivi di interesse pubblico") e lettera a) ("consenso esplicito").

63. La pandemia causata dal COVID-19 sta provocando una crisi sanitaria eccezionale e senza precedenti in termini di natura e portata. In tale contesto, il Comitato ritiene che la lotta al COVID-19 sia stata riconosciuta dall'UE e dalla maggior parte dei suoi Stati membri come un interesse pubblico rilevante[26], tale da richiedere un'azione urgente nel campo della ricerca scientifica (ad esempio per individuare trattamenti e/o sviluppare vaccini) e comportare anche trasferimenti di dati verso paesi terzi o organizzazioni internazionali.[27]

64. Non solo le autorità pubbliche, ma anche i soggetti privati che contribuiscono al perseguimento di tale interesse pubblico (ad esempio, un istituto di ricerca universitario che collabori alla messa a punto di un vaccino nell'ambito di un partenariato internazionale) potrebbero, nell'attuale contesto di pandemia, avvalersi della deroga di cui sopra.

65. Inoltre, in determinate circostanze, in particolare quando i trasferimenti siano effettuati da soggetti privati per scopi di ricerca medica finalizzata a combattere la pandemia da COVID-19,[28] tali trasferimenti di dati personali potrebbero avvenire in via alternativa sulla base del consenso esplicito degli interessati.[29]

66. Nel contesto dell'attuale pandemia, ove non sia possibile basarsi su una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o su garanzie adeguate ai sensi dell'articolo 46, le autorità pubbliche e i soggetti privati possono ricorrere alle deroghe applicabili di cui sopra, principalmente come misura temporanea giustificata dall'urgenza della situazione sanitaria a livello mondiale.

67. In effetti, se è vero che la natura della crisi dovuta al COVID-19 può giustificare il ricorso alle deroghe applicabili con riguardo ai trasferimenti iniziali effettuati a fini di ricerca in questo contesto, trasferimenti ripetuti di dati verso paesi terzi nel quadro di un progetto di ricerca di lungo periodo dovrebbero essere assistiti da garanzie adeguate ai sensi dell'articolo 46 del RGPD.[30]

68. Infine, con riguardo a tali trasferimenti va osservato che si dovranno analizzare, caso per caso, i ruoli rispettivamente ricoperti (titolare del trattamento, responsabile del trattamento, co-titolare) e gli obblighi in capo ai singoli attori coinvolti (sponsor, sperimentatori) al fine di individuare le misure per un idoneo inquadramento delle operazioni di trasferimento.

8. SINTESI

69. Le principali indicazioni ricavabili dalle presenti Linee guida sono così sintetizzabili:

1. Il regolamento generale sulla protezione dei dati prevede norme speciali per il trattamento dei dati relativi alla salute a fini di ricerca scientifica, applicabili anche nel contesto della pandemia da COVID-19.
2. Il legislatore nazionale di ciascuno Stato membro ha il potere di emanare norme specifiche ai sensi dell'articolo 9, paragrafo 2, lettere i) e j), del RGPD al fine di consentire il trattamento dei dati relativi alla salute a fini di ricerca scientifica. Il trattamento dei dati relativi alla salute a fini di ricerca scientifica deve altresì fondarsi su una delle basi giuridiche di cui all'articolo 6, paragrafo 1, del RGPD. Pertanto, le condizioni e la portata di tale trattamento variano a seconda del diritto del singolo Stato membro.
3. Tutte le norme adottate in base all'articolo 9, paragrafo 2, lettera i) e lettera j), del RGPD devono essere interpretate alla luce dei principi dell'articolo 5 del RGPD e della giurisprudenza della Corte di giustizia. In particolare, le deroghe e le limitazioni relative alla protezione dei dati di cui all'articolo 9, paragrafo 2, lettera j), e all'articolo 89, paragrafo 2, del RGPD devono applicarsi solo nella misura strettamente necessaria.
4. Tenuto conto dei rischi di trattamento nel contesto dell'epidemia dovuta a COVID-19, occorre porre l'accento sull'osservanza dell'articolo 5, paragrafo 1, lettera f), dell'articolo 32, paragrafo 1, e dell'articolo 89, paragrafo 1, del RGPD. Occorre stabilire se sia necessario effettuare una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del RGPD.
5. Si devono stabilire periodi di conservazione e tali periodi devono essere proporzionati. In questo contesto, dovrebbero essere presi in considerazione criteri quali la durata e lo scopo della ricerca. Le disposizioni nazionali possono disciplinare anche il periodo di conservazione, e di ciò occorre tenere conto.
6. In linea di principio, situazioni quali l'attuale emergenza dovuta al COVID-19 non sospendono né limitano la possibilità degli interessati di esercitare i loro diritti ai sensi degli articoli 12-22 del RGPD. Tuttavia, l'articolo 89, paragrafo 2, del RGPD consente al legislatore nazionale di limitare (in alcuni casi) i diritti dell'interessato di cui al capo 3 del regolamento. Di conseguenza, possono aversi *differenti* limitazioni dei diritti degli interessati a seconda del diritto del singolo Stato membro.
7. Per quanto riguarda i trasferimenti internazionali, in assenza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, del RGPD o di garanzie adeguate ai sensi dell'articolo 46 di quest'ultimo, i soggetti pubblici e privati possono avvalersi delle deroghe applicabili a norma dell'articolo 49 del RGPD. Tuttavia, le deroghe di cui all'articolo 49 del RGPD hanno natura assolutamente eccezionale.

Per il comitato europeo per la protezione dei dati
La Presidente

Andrea Jelinek

NOTE

[1] Si veda la dichiarazione del comitato europeo per la protezione dei dati del 19.3.2020 sul trattamento dei dati personali nel contesto del focolaio di COVID-19, disponibile all' indirizzo https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en (versione italiana: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9295504).

[2] Vedi ad esempio l'articolo 5, paragrafo 1, lettera b) e lettera e), l'articolo 14, paragrafo 5, lettera b), e l'articolo 17, paragrafo 3, lettera d), del RGPD.

[3] Vedi ad esempio l'articolo 9, paragrafo 2, lettera j), e l'articolo 89, paragrafo 2, del RGPD.

[4] Vedi ad esempio, con riguardo alla direttiva 95/46/CE, la causa C-101/01, 6.11.2003 (Lindqvist), punto 50.

[5] Si vedano le linee guida sul consenso a norma del regolamento (Ue) n. 2016/679 del 10.04.2018 approvate dal Gruppo di lavoro « Articolo 29 » WP259 rev.01, pag. 27 (adottate dal Comitato europeo per la protezione dei dati). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id = 623051.

[6] Vedi, ad esempio, per quanto riguarda la direttiva 95/46/CE, la decisione della CGUE del 13.5.2014, C-131/12 (Google Spain), punto 71.

[7] Si veda il parere 3/2019 del Comitato europeo per la protezione dei dati, del 23.1.2019, relativo alle FAQ sull'interazione tra il regolamento sulla sperimentazione clinica (CTR) e il regolamento generale sulla protezione dei dati (RGPD), https://edpb.europa.eu/our-work-tools/our-documents/avis-art-70/opinion-32019-concerning-questions-and-answers-interplay_en.

[8] Linee guida in materia di consenso a norma del regolamento (UE) n. 2016/679 del Gruppo di lavoro « Articolo 29 » del 10.04.2018, WP259 rev.01, pag. 18 (adottate dal Comitato europeo per la protezione dei dati).

[9] Sul presupposto che l'interessato non sia stato oggetto di pressioni né debba paventare conseguenze negative in caso non intenda prestare il proprio consenso.

[10] Vedi articolo 17, paragrafo 1, lettera b), e paragrafo 3, del RGPD.

[11] Si veda il parere 3/2019 del Comitato europeo per la protezione dei dati del 23.1.2019, pag. 7.

[12] Si veda ad esempio, relativamente alla direttiva 95/46/CE, la sentenza della Corte di giustizia europea del 14.2.2019, C-345/17 (Buivids), paragrafo 64.

[13] Linee guida sulla trasparenza a norma del regolamento (UE) n. 2016/679 del Gruppo di lavoro « Articolo 29 », WP260 rev.01, pag. 29 (adottate dal Comitato europeo per la protezione dei dati) :https://ec.europa.eu/newsroom/article29/item-detail.cfm?item id = 622227.

[14] Linee guida sulla trasparenza a norma del regolamento (UE) n. 2016/679 del Gruppo di lavoro « Articolo 29 », WP260 rev.01, pag. 31 (adottate dal Comitato europeo per la protezione dei dati)

[15] Linee guida sulla trasparenza a norma del regolamento (UE) n. 2016/679 del Gruppo di lavoro « Articolo 29 », WP260 rev.01, pag. 32 (adottate dal Comitato europeo per la protezione dei dati).

[16] Si vedano anche le Linee guida 4/2019 del Comitato (13.11.2019) sulla protezione dei dati fin dalla progettazione e per impostazione predefinita: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en .

[17] Si osservi che i dati personali (relativi alla salute) pseudonimizzati sono considerati ancora "dati personali" ai sensi dell'articolo 4, paragrafo 1, del Regolamento e non devono essere confusi con "dati anonimizzati" che invece non consentono alcun collegamento con singoli interessati. Cfr., ad esempio, il considerando 28.

[18] Vedi, ad esempio, con riguardo alla direttiva 95/46/CE, la sentenza della Corte di giustizia europea del 14.2.2019, C-345/17 (Buivids), paragrafo 64.

[19] Articolo 44, RGPD.

[20] Vedi i punti da 4 a 6 delle presenti Linee guida.

[21] Si vedano le Linee guida 2/2018 del Comitato europeo per la protezione dei dati del 25.5.2018, sulle deroghe di cui all'articolo 49 del regolamento (UE) n. 2016/679, pag. 3, a proposito della verifica in due fasi: https://edpb.europa.eu/

our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_en .

[22] I trasferimenti internazionali di dati possono essere un fattore di rischio da considerare nell'ambito di una valutazione d'impatto sulla protezione dei dati di cui alla pagina 10 delle presenti Linee guida.

[23] L'elenco dei paesi riconosciuti adeguati dalla Commissione europea è disponibile all'indirizzo https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisioni.

[24] Quali, ad esempio, clausole tipo di protezione dei dati a norma dell'articolo 46, paragrafo 2, lettera c) o d), del RGPD; clausole contrattuali ad hoc a norma dell'articolo 46, paragrafo 3, lettera a), del RGPD; disposizioni amministrative ai sensi dell'articolo 46, paragrafo 3, lettera b), del RGPD.

[25] Vedi le Linee guida 2/2018, pag. 3.

[26] L'articolo 168 del Trattato sul funzionamento dell'Unione europea riconosce un livello elevato di protezione della salute umana quale obiettivo importante che dovrebbe essere garantito nell'attuazione di tutte le politiche e attività dell'Unione. Su tale base, l'azione dell'Unione sostiene le politiche nazionali volte a migliorare la salute pubblica, anche nella lotta contro i grandi flagelli sanitari e le gravi minacce per la salute a carattere transfrontaliero, ad esempio promuovendo la ricerca sulle loro cause, la loro trasmissione e la loro prevenzione. Analogamente, i considerando 46 e 112 del RGPD menzionano il trattamento effettuato nel contesto della lotta contro le epidemie come esempio di trattamento per importanti motivi di interesse pubblico. Nel contesto della pandemia da COVID-19, l'UE ha adottato una serie di misure in un'ampia gamma di settori (ad esempio il finanziamento dei sistemi sanitari, il sostegno ai pazienti transfrontalieri e l'impiego di personale medico, l'assistenza finanziaria agli indigenti, i trasporti, i dispositivi medici, ecc.) sul presupposto che l'UE deve affrontare un'importante emergenza sanitaria pubblica che richiede una risposta urgente.

[27] Il Comitato sottolinea che il regolamento generale sulla protezione dei dati, al considerando 112, menziona lo scambio internazionale di dati tra servizi competenti per la sanità pubblica quale esempio dell'applicazione di tale deroga.

[28] Conformemente all'articolo 49, paragrafo 3, del RGPD, il consenso non può essere utilizzato per le attività svolte da autorità pubbliche nell'esercizio di pubblici poteri.

[29] Si vedano le Linee guida del Comitato europeo per la protezione dei dati 2/2018, sezione 2.1.

[30] Si vedano le Linee guida del Comitato europeo per la protezione dei dati 2/2018, pag. 5.

Linee guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19

Adottate il 21 aprile 2020

Cronologia delle versioni

Versione 1.1	5 maggio 2020	Piccole correzioni
Versione 1.0	21 aprile 2020	Adozione delle Linee guida

Indice

1 INTRODUZIONE & CONTESTO

2 UTILIZZO DEI DATI RELATIVI ALL'UBICAZIONE

3 APP PER IL TRACCIAMENTO DEI CONTATTI

4 CONCLUSIONE

ALLEGATO - APPLICAZIONI PER IL TRACCIAMENTO DEI CONTATTI
GUIDA ALL'ANALISI

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

Visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in prosieguo "RGPD"),

Visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificato dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio[1] 2018,

Visti l'articolo 12 e l'articolo 22 del suo regolamento,

ADOTTA LE SEGUENTI LINEE GUIDA:

1. INTRODUZIONE & CONTESTO

1. Governi e soggetti privati si stanno orientando verso l'uso di soluzioni basate sui dati nell'ambito della risposta alla pandemia causata dal COVID-19, e ciò suscita numerose preoccupazioni in materia di tutela della vita privata.
2. Il Comitato europeo per la protezione dei dati sottolinea che il quadro giuridico in materia di protezione dei dati è stato concepito per essere flessibile e, in quanto tale, è in grado di conseguire una risposta efficace per limitare la pandemia e proteggere i diritti umani e le libertà fondamentali.
3. Il Comitato è fermamente convinto che, ove sia necessario ricorrere al trattamento di dati personali per gestire la pandemia causata dal COVID-19, la protezione dei dati è indispensabile per generare un clima di fiducia, creare le condizioni per l'accettabilità sociale di qualsiasi soluzione e garantire, pertanto, l'efficacia di tali misure. Poiché il virus non conosce confini, appare preferibile sviluppare un approccio comune europeo in risposta alla crisi attuale, o almeno realizzare una cornice di interoperabilità.
4. Il Comitato ritiene, in via generale, che i dati e le tecnologie utilizzati per contribuire alla lotta al COVID-19 debbano servire a dare maggiori strumenti alle persone, piuttosto che a controllarle, stigmatizzarle o reprimerne i comportamenti. Inoltre, mentre i dati e le tecnologie possono essere strumenti importanti, essi hanno limiti intrinseci e non possono che far leva sull'efficacia di altre misure di sanità pubblica. I principi generali di efficacia, necessità e proporzionalità devono guidare qualsiasi misura adottata dagli Stati membri o dalle istituzioni dell'UE che comporti il trattamento di dati personali per combattere il COVID-19.

- Le presenti linee guida chiariscono le condizioni e i principi per l'uso proporzionato dei dati di localizzazione e degli strumenti di tracciamento dei contatti, in due ambiti specifici :
- Utilizzo dei dati di localizzazione a supporto della risposta alla pandemia tramite la definizione di modelli della diffusione del virus, al fine di valutare l'efficacia complessiva di misure di isolamento e quarantena;

5. Utilizzo del tracciamento dei contatti per informare le persone che sono probabilmente entrate in contatto ravvicinato con soggetti successivamente confermati positivi, al fine di interrompere tempestivamente la trasmissione del contagio.
6. L'efficienza del contributo che le app per il tracciamento dei contatti possono fornire alla gestione della pandemia dipende da molti fattori (ad esempio, percentuale di persone che dovrebbero installarle; definizione di "contatto" in termini di prossimità e durata). Inoltre, tali applicazioni devono far parte di una strategia globale in materia di sanità pubblica per combattere la pandemia, compresi, tra l'altro, la sperimentazione e il successivo tracciamento manuale dei contatti ai fini dell'eliminazione di casi dubbi. La loro diffusione dovrebbe essere accompagnata da misure di sostegno volte a garantire che le informazioni fornite agli utenti siano contestualizzate e che le segnalazioni possano essere utili al sistema sanitario pubblico. In caso contrario,

queste applicazioni potrebbero non esplicare appieno la propria efficacia.

7. Il Comitato sottolinea che il regolamento generale sulla protezione dei dati (RGPD) e la direttiva 2002/58/CE (la "direttiva relativa alla vita privata e alle comunicazioni elettroniche", direttiva e-privacy) contengono norme specifiche che consentono l'uso di dati anonimi o personali per sostenere le autorità pubbliche e altri soggetti, a livello nazionale e dell'UE, nel monitoraggio e nel contenimento della diffusione del virus SAR-CoV-2[2].

8. A tale riguardo, il Comitato si è già pronunciato sul fatto che il ricorso alle app per il tracciamento dei contatti dovrebbe essere volontario e non dovrebbe basarsi sulla tracciabilità dei movimenti individuali, bensì sulle informazioni di prossimità relative agli utenti.[3]

2. UTILIZZO DEI DATI RELATIVI ALL'UBICAZIONE

2.1 FONTI DEI DATI RELATIVI ALL'UBICAZIONE

9. Per la modellizzazione della diffusione del virus e dell'efficacia complessiva delle misure di confinamento, esistono due principali fonti di dati relativi all'ubicazione:

- dati relativi all'ubicazione raccolti da fornitori di servizi di comunicazione elettronica (come gli operatori di telecomunicazioni mobili) nel corso della prestazione del loro servizio; e
- dati relativi all'ubicazione raccolti da fornitori di servizi della società dell'informazione, la cui funzionalità richiede l'uso di tali dati (ad esempio, navigazione, servizi di trasporto, ecc.).

10. Il Comitato ricorda che i dati relativi all'ubicazione[4] raccolti dai fornitori di comunicazioni elettroniche possono essere trattati solo entro i limiti di cui agli articoli 6 e 9 della direttiva relativa alla vita privata e alle comunicazioni elettroniche. Ciò significa che tali dati possono essere trasmessi alle autorità o a terzi solo se sono stati resi anonimi dal fornitore oppure, per i dati indicanti la posizione geografica dell'apparecchiatura terminale di un utente, che non sono dati relativi al traffico, con il consenso previo degli utenti[5].

11. Per quanto riguarda le informazioni, compresi i dati relativi all'ubicazione, raccolte direttamente dall'apparecchiatura terminale, si applica l'articolo 5 (3) della direttiva relativa alla vita privata e alle comunicazioni elettroniche. Pertanto, l'archiviazione di informazioni sul dispositivo dell'utente o l'accesso alle informazioni già archiviate sono consentiti solo se i) l'utente ha prestato il consenso[6] o ii) la memorizzazione e/o l'accesso sono strettamente necessari al servizio della società dell'informazione esplicitamente richiesto dall'utente.

12. Sono tuttavia possibili, a norma dell'articolo 15 della direttiva relativa alla vita privata e alle comunicazioni elettroniche, deroghe ai diritti e agli obblighi previsti quando tali deroghe costituiscono una misura necessaria, adeguata e proporzionata all'interno di una società democratica per determinati obiettivi[7].

13. Per quanto riguarda il riutilizzo dei dati di localizzazione raccolti da un fornitore di servizi della società dell'informazione a fini di modellizzazione (ad esempio attraverso il sistema operativo o alcune applicazioni precedentemente installate), devono essere soddisfatte ulteriori condizioni. In effetti, quando i dati sono stati raccolti in conformità all'articolo 5 (3) della direttiva relativa alla vita privata e alle comunicazioni elettroniche, essi possono essere trattati ulteriormente solo con il consenso supplementare dell'interessato o sulla base di una normativa dell'Unione o di uno Stato membro che costituisce una misura necessaria e proporzionata, in una società democratica, per salvaguardare gli obiettivi di cui all'articolo 23 (1) del RGPD.[8]

2.2 UTILIZZO DI DATI ANONIMIZZATI RELATIVI ALL'UBICAZIONE

14. Il Comitato sottolinea che, per quanto riguarda l'utilizzo dei dati relativi all'ubicazione, occorre sempre privilegiare il trattamento di dati anonimi piuttosto che di dati personali.
15. L'anonimizzazione fa riferimento all'uso di una serie di tecniche finalizzate a eliminare la possibilità di collegare i dati a una persona fisica identificata o identificabile con uno sforzo "ragionevole". Questo "test di ragionevolezza" deve tenere conto sia degli aspetti oggettivi (tempi, mezzi tecnici) sia di elementi di contesto che possono variare caso per caso (rarità di un fenomeno alla luce, per esempio, della densità di popolazione, la natura e il volume dei dati). Se i dati non superano tale test, non sono anonimizzati e pertanto rientrano nel campo di applicazione del regolamento generale sulla protezione dei dati.
16. La valutazione della robustezza della tecnica di anonimizzazione adottata dipende da tre fattori: (i) individuabilità (singling out) (possibilità di isolare una persona all'interno di un gruppo sulla base dei dati); (ii) correlabilità (possibilità di correlare due record riguardanti la stessa persona); (iii) inferenza (possibilità di dedurre, con probabilità significativa, informazioni sconosciute relative a una persona).
17. Il concetto di anonimizzazione tende ad essere frainteso e spesso confuso con la pseudonimizzazione. Mentre l'anonimizzazione consente di utilizzare i dati senza restrizioni, i dati pseudonimizzati rientrano nel campo di applicazione del regolamento generale sulla protezione dei dati.
18. Esistono molte opzioni per conseguire un'anonimizzazione efficace[9], ma con un caveat. I dati non possono essere resi anonimi isolatamente, il che significa che solo intere serie o interi insiemi di dati sono passibili di anonimizzazione. In tal senso, qualsiasi intervento su un dato isolato o sulla serie storica di dati riferibili a un singolo interessato (mediante cifratura o altre trasformazioni matematiche) può essere considerato, nel migliore dei casi, una pseudonimizzazione.
19. I processi di anonimizzazione e i tentativi di re-identificazione sono oggetto di numerosi studi e ricerche. È fondamentale che ogni titolare che implementi soluzioni di anonimizzazione si mantenga aggiornato sugli sviluppi recenti in questo campo, in particolare per quanto riguarda i dati relativi all'ubicazione

(provenienti da operatori delle telecomunicazioni e/o da servizi della società dell'informazione) che sono notoriamente difficili da anonimizzare.

20. In effetti, un ampio corpus di ricerche ha dimostrato[10] che *dati relativi all'ubicazione ritenuti anonimi* possono di fatto non esserlo. Le tracce di mobilità dei singoli individui sono caratterizzate intrinsecamente da forte correlazione e univocità. Pertanto, in determinate circostanze possono essere vulnerabili ai tentativi di re-identificazione.

21. Un'unica serie di dati che consenta di rintracciare l'ubicazione di un individuo lungo un arco di tempo significativo non può essere pienamente anonimizzata. Questa affermazione resta valida se non si riduce in misura sufficiente la precisione delle coordinate geografiche registrate, o se non si eliminano dettagli del percorso di tracciamento, e anche se si mantiene solo l'ubicazione dei luoghi in cui l'interessato permane per un tempo considerevole. E vale anche in caso di insufficiente aggregazione dei dati relativi all'ubicazione.

22. Al fine di conseguire l'anonimizzazione, i dati relativi all'ubicazione devono essere trattati con attenzione per soddisfare il test di ragionevolezza. In tal senso, il trattamento deve prendere in considerazione gli insiemi di dati di ubicazione nel loro complesso, e riguardare dati di una serie ragionevolmente ampia di individui utilizzando tecniche di anonimizzazione disponibili e con caratteristiche robuste, implementandole in modo adeguato ed efficace.

23. Infine, data la complessità dei processi di anonimizzazione, si raccomanda con forza di garantire la trasparenza per quanto riguarda la metodologia di anonimizzazione utilizzata.

3. APP PER IL TRACCIAMENTO DEI CONTATTI

3.1 ANALISI GIURIDICA GENERALE

24. Il monitoraggio sistematico e su larga scala dell'ubicazione e/o dei contatti tra persone fisiche costituisce una grave interferenza nella vita privata. Essa può essere legittimata solo facendo affidamento su un'adozione volontaria da parte degli utenti per ciascuno dei rispettivi scopi. Ciò implica, in particolare, che le persone che non intendono o non possono utilizzare tali applicazioni non dovrebbero subire alcun pregiudizio.

25. Per garantire il rispetto del principio di responsabilizzazione, dovrebbe essere definita chiaramente la titolarità del trattamento di un'eventuale app per il tracciamento di contatti. Il Comitato ritiene che le autorità sanitarie nazionali possano essere i titolari di tale trattamento[11]; si possono comunque prendere in considerazione altre configurazioni di titolarità. In ogni caso, se il processo di diffusione delle app per il tracciamento dei contatti coinvolge diversi attori, devono essere definiti con chiarezza e fin dall'inizio i ruoli e le responsabilità rispettive e di tutto ciò devono essere informati gli utenti.

26. Inoltre, per quanto riguarda il principio della limitazione delle finalità, le finalità devono essere sufficientemente specifiche così da escludere tratta-

menti ulteriori per scopi non correlati alla gestione della crisi sanitaria causata da COVID-19 (ad esempio, per fini commerciali o per le attività di contrasto di matrice giudiziaria o di polizia). Una volta definita con chiarezza la finalità, sarà necessario garantire che l'uso dei dati personali sia adeguato, necessario e proporzionato.

27. Nel contesto di un'app per il tracciamento dei contatti, occorre prestare particolare attenzione al principio di minimizzazione e ai principi della protezione dei dati fin dalla progettazione e per impostazione predefinita (*data protection by design and by default*):

- le app per il tracciamento dei contatti non necessitano del tracciamento della posizione dei singoli utenti. Occorre invece utilizzare i dati di prossimità;
- poiché le app per il tracciamento dei contatti possono funzionare senza l'identificazione diretta delle persone, dovrebbero essere adottate misure adeguate per prevenire la reidentificazione;
- le informazioni raccolte dovrebbero risiedere nell'apparecchiatura terminale dell'utente e dovrebbero essere raccolte solo le informazioni pertinenti e solo ove strettamente necessarie.

28. Per quanto riguarda la liceità del trattamento, il Comitato rileva che le app per il tracciamento dei contatti comportano la memorizzazione e/o l'accesso a informazioni già archiviate nell'apparecchiatura terminale dell'utente, che sono soggette all'articolo 5 (3) della direttiva ePrivacy. Se tali operazioni sono strettamente necessarie per consentire al fornitore dell'app di rendere il servizio esplicitamente richiesto dall'utente, il trattamento non richiede il consenso di quest'ultimo. Per le operazioni che non sono strettamente necessarie, il fornitore dovrebbe richiedere il consenso dell'utente.

29. Inoltre, il Comitato osserva come la circostanza per cui l'uso di app per il tracciamento dei contatti avvenga su base volontaria non implichi che il trattamento dei dati personali debba necessariamente basarsi sul consenso. Qualora autorità pubbliche forniscano un servizio sulla base di un mandato conferito dalla legge e conformemente ai requisiti stabiliti da tale legge, la base giuridica più pertinente risulta essere la necessità del trattamento per lo svolgimento di un compito di interesse pubblico, ossia l'articolo 6, paragrafo 1, lettera e), del Regolamento generale sulla protezione dei dati.

30. L'articolo 6, paragrafo 3, del Regolamento precisa che la base su cui si fonda il trattamento di cui all'articolo 6, paragrafo 1, lettera e) è stabilita dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare. La finalità del trattamento è definita in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.[12]

31. Tuttavia, la base giuridica o la misura legislativa che costituisce il fondamento di liceità per l'uso dell'app di tracciamento dei contatti dovrebbero prevedere garanzie significative, compreso un riferimento alla natura volontaria dell'app. Dovrebbe essere inclusa una chiara specificazione delle finalità e delle limitazioni riguardanti l'ulteriore utilizzo dei dati personali, nonché

una chiara identificazione del titolare o dei titolari coinvolti. Occorre inoltre individuare le categorie di dati e i soggetti ai quali i dati personali possono essere comunicati, e per quali scopi. A seconda del grado di interferenza, occorre integrare salvaguardie ulteriori tenendo conto della natura, della portata e delle finalità del trattamento. Infine, il Comitato raccomanda di prevedere, non appena possibile, i criteri per stabilire quando l'app dovrà essere disinstallata e a chi spetti assumere tale determinazione.

32. Tuttavia, se il trattamento dei dati si basa su una diversa base giuridica, quale[13] ad esempio il consenso (articolo 6 (1) (a)), il titolare dovrà garantire che siano soddisfatti i requisiti rigorosi previsti per tale base giuridica.

33. Inoltre, il ricorso a un'app per combattere la pandemia da COVID-19 potrebbe portare alla raccolta di dati relativi alla salute (ad esempio lo status di persona infetta). Il trattamento di tali dati è consentito quando è necessario per motivi di interesse pubblico nel settore della sanità pubblica, nel rispetto delle condizioni di cui all'articolo 9, paragrafo 2, lettera i), del Regolamento[14], o per le finalità dell'assistenza sanitaria di cui all'articolo 9, paragrafo 2, lettera h), del Regolamento stesso[15]. A seconda della base giuridica individuata, il trattamento in questione potrebbe anche fondarsi sul consenso esplicito dell'interessato (articolo 9, paragrafo (2), lettera a), del Regolamento).

34. Conformemente allo scopo iniziale, l'articolo 9, paragrafo 2, lettera j), del Regolamento consente inoltre che i dati relativi alla salute siano trattati ove necessario a fini di ricerca scientifica o a fini statistici.

35. L'attuale crisi sanitaria non dovrebbe trasformarsi in un'occasione per derogare rispetto al principio di limitazione della conservazione dei dati. La conservazione dovrebbe essere limitata alla luce delle reali esigenze e della rilevanza medica (anche con riguardo a considerazioni di natura epidemiologica quali il periodo di incubazione, ecc.) e i dati personali dovrebbero essere conservati solo per la durata della crisi dovuta al COVID-19. Successivamente, di norma, tutti i dati personali dovrebbero essere cancellati o resi anonimi.

36. Il Comitato ritiene che tali app non possano sostituire, ma solo supportare, il tracciamento manuale dei contatti effettuato da personale sanitario pubblico qualificato, che potrà stabilire con quale probabilità contatti ravvicinati diano luogo a una trasmissione del virus o meno (ad esempio, in caso di interazioni con una persona protetta da un adeguato equipaggiamento, come può avvenire ad esempio per un addetto alla cassa di un supermercato ecc.). Il Comitato sottolinea che tutte le procedure e i processi, compresi gli algoritmi implementati dalle app per il tracciamento dei contatti, dovrebbero svolgersi sotto la stretta sorveglianza di personale qualificato al fine di limitare il verificarsi di falsi positivi e negativi. In particolare, le indicazioni fornite in merito ai passi da compiere successivamente alla ricezione di un alert non dovrebbero basarsi unicamente su un trattamento automatizzato.

37. Al fine di garantire la correttezza dei trattamenti, il rispetto del principio di responsabilizzazione e, più in generale, la conformità con la legge, gli algoritmi devono essere verificabili e devono essere soggetti a un riesame periodico da parte di esperti indipendenti. Il codice sorgente dovrebbe essere reso pubblico così da assicurare la più ampia trasparenza possibile.

38. Vi sarà sempre, in una certa misura, la possibilità del verificarsi di falsi positivi. Poiché l'identificazione di un rischio di infezione può avere un forte impatto sui singoli individui, ad esempio imponendo l'autoisolamento fino a negativizzazione del test, è indispensabile poter effettuare correzioni dei dati e/o dei risultati delle analisi successive. Naturalmente ciò vale solo in presenza di situazioni o implementazioni in cui il trattamento e la conservazione dei dati sono configurati in modo da permettere tecnicamente di apportare le correzioni suddette, e ove sia probabile il verificarsi degli effetti negativi di cui sopra.

39. Infine, il Comitato ritiene che debba essere effettuata una valutazione d'impatto sulla protezione dei dati prima di implementare le app in questione, in quanto il trattamento configura una probabilità di rischio elevato (dati relativi alla salute, adozione prevista su larga scala, monitoraggio sistematico, uso di una nuova soluzione tecnologica)[16]. Il Comitato raccomanda vivamente la pubblicazione degli esiti di tali valutazioni.

3.2 RACCOMANDAZIONI E REQUISITI FUNZIONALI

40. Conformemente al principio di minimizzazione, tra le altre misure in ossequio al principio di protezione dei dati fin dalla progettazione e per impostazione predefinita[17], i dati trattati dovrebbero essere limitati a quelli strettamente necessari. L'app non dovrebbe raccogliere informazioni non correlate o non necessarie come, per esempio, dati anagrafici, identificativi di comunicazione, voci di directory del dispositivo, messaggi, registrazioni di chiamate, dati relativi all'ubicazione, identificativi del dispositivo, ecc. .

41. I dati trasmessi dall'app devono includere solo identificatori univoci e pseudonimi, generati dall'app e specifici di tale app. Tali identificatori devono essere rinnovati regolarmente, secondo una frequenza compatibile con lo scopo di contenere la diffusione del virus e sufficiente a limitare il rischio di identificazione e di localizzazione fisica delle persone.

42. Le applicazioni per il tracciamento dei contatti possono seguire un approccio centralizzato o decentrato[18]. Entrambe le opzioni sono praticabili, a condizione che siano in vigore adeguate misure di sicurezza, ed entrambe comportano una serie di vantaggi e svantaggi. Pertanto, la fase di progettazione delle app dovrebbe sempre prevedere un esame approfondito di entrambi gli approcci, ponderandone attentamente gli effetti in termini di protezione dei dati e privacy nonché i possibili impatti sui diritti delle persone.

43. Ogni server coinvolto nel sistema di tracciamento dei contatti deve raccogliere soltanto la cronologia dei contatti o gli identificativi pseudonimizzati di un utente diagnosticato come infetto a seguito di un'adeguata valutazione effettuata dalle autorità sanitarie e di un'azione volontaria dell'utente stesso. Alternativamente, il server deve conservare un elenco degli identificativi pseudonimizzati di utenti infetti o la rispettiva cronologia dei contatti solo per il periodo necessario a informare gli utenti potenzialmente infetti della loro avvenuta esposizione, senza tentare di individuare tali utenti potenzialmente infetti.

44. La realizzazione di una complessiva strategia di tracciamento dei contatti comprendente sia l'impiego di app sia il tracciamento manuale può richiedere, in alcuni casi, il trattamento di ulteriori informazioni. In questo caso, tali informazioni supplementari dovrebbero rimanere nel dispositivo dell'utente e saranno trattate solo ove strettamente necessario e con il previo e specifico consenso dell'utente stesso.
45. Si deve fare ricorso a tecniche crittografiche di ultima generazione per garantire la conservazione sicura dei dati memorizzati nei server e nelle app, nonché gli scambi tra le app e il server remoto. Occorre inoltre implementare sistemi di autenticazione reciproca tra l'app e il server.
46. La segnalazione nell'app di utenti infetti da SARS-CoV-2 deve essere soggetta a idonea procedura, ad esempio mediante l'impiego di un codice monouso correlato a una identità pseudonima della persona infetta e collegato a un laboratorio o a un operatore sanitario. Se la conferma non può essere ottenuta in modo sicuro, non dovrebbe aversi alcun trattamento di dati sulla base di una presunzione di validità dello status relativo all'utente.
47. Il titolare del trattamento, in collaborazione con le autorità pubbliche, deve fornire informazioni chiare e inequivocabili sul link ove scaricare l'app ufficiale per il tracciamento dei contatti al fine di ridurre il rischio che gli utenti utilizzino un'app di terze parti.

4. CONCLUSIONE

48. Il mondo si trova ad affrontare una grave crisi sanitaria che richiede risposte forti, il cui impatto si manifesterà anche oltre il termine di questa emergenza. Il trattamento automatizzato dei dati e le tecnologie digitali possono essere elementi chiave nella lotta al COVID-19. Tuttavia, occorre guardarsi dal rischio di effetti irreversibili. Spetta a noi tutti garantire che ogni misura adottata in queste circostanze eccezionali sia necessaria, limitata nel tempo, di portata minima e soggetta a un riesame periodico ed effettivo nonché a una valutazione scientifica.
49. Il Comitato europeo per la protezione dei dati sottolinea che a nessuno dovrebbe essere chiesto di scegliere tra una risposta efficace all'attuale crisi e la tutela dei diritti fondamentali: entrambi gli obiettivi sono alla nostra portata, e i principi di protezione dei dati possono svolgere un ruolo molto importante nella lotta contro il virus. Il diritto europeo in materia di protezione dei dati consente l'uso responsabile dei dati personali per la gestione della salute, garantendo al contempo che non siano erosi i diritti e le libertà individuali.

Per il Comitato europeo per la protezione dei dati
La Presidente

Andrea Jelinek

ALLEGATO - APPLICAZIONI PER IL TRACCIAMENTO DEI CONTATTI GUIDA ALL'ANALISI

0. AVVERTENZA

I seguenti orientamenti non sono né prescrittivi né esaustivi e intendono unicamente fornire indicazioni generali per sviluppatori e realizzatori di app di tracciamento dei contatti. Soluzioni diverse da quelle qui descritte sono ammesse e lecite purché conformi al pertinente quadro giuridico (il Regolamento generale sulla protezione dei dati e la Direttiva e-privacy).

Si osservi, inoltre, che la presente guida ha natura generale. Di conseguenza, le raccomandazioni e gli obblighi contenuti nel presente documento non devono essere considerati esaustivi. Le valutazioni devono essere effettuate caso per caso; inoltre, determinate app possono richiedere misure supplementari non comprese nelle indicazioni qui fornite.

1. SINTESI

In molti Stati membri si valuta il ricorso ad applicazioni (app) di *tracciamento dei contatti* per facilitare l'individuazione di eventuali contatti con una persona affetta da SARS-Cov-2.

Non sono ancora definite le condizioni alle quali tali app contribuirebbero efficacemente alla gestione della pandemia, e tale definizione dovrebbe costituire un presupposto necessario per l'implementazione di un'app del tipo descritto. Tuttavia, è opportuno fornire linee guida che, in via preliminare, diano indicazioni pertinenti ai team di sviluppatori in modo da assicurare la protezione dei dati personali fin dalla fase iniziale di progettazione.

Si osservi, inoltre, che la presente guida ha natura generale. Di conseguenza, le raccomandazioni e gli obblighi contenuti nel presente documento non devono essere considerati esaustivi. Le valutazioni devono essere effettuate caso per caso; inoltre, determinate app possono richiedere misure supplementari non comprese nelle indicazioni qui elaborate. Scopo della presente guida è fornire orientamenti generali per sviluppatori e realizzatori di app di tracciamento dei contatti.

Alcuni criteri potrebbero andare al di là dei requisiti strettamente derivanti dal quadro normativo in materia di protezione dei dati. Tali criteri mirano a garantire il massimo livello di trasparenza al fine di favorire l'accettazione sociale delle app di tracciamento dei contatti.

A tal fine, i soggetti che rilasciano sul mercato app di tracciamento dei contatti dovrebbero tener conto dei seguenti criteri:

- L'uso dell'app deve essere rigorosamente volontario e non può costituire condizione per l'esercizio dei diritti previsti dalla legge. Le persone devono

avere il pieno controllo dei propri dati in ogni momento e devono poter scegliere liberamente se utilizzare l'app o meno.

- Le app di tracciamento dei contatti possono comportare un rischio elevato per i diritti e le libertà delle persone fisiche e, quindi, è necessaria una valutazione d'impatto sulla protezione dei dati prima della loro introduzione.
- È possibile ottenere informazioni sulla prossimità tra utenti dell'app senza geolocalizzarli. Questo tipo di app non necessita di dati relativi all'ubicazione e, pertanto, non deve comportarne l'utilizzo.
- A seguito della diagnosi di infezione da SARS-Cov-2 concernente un utente, dovrebbero essere informate solo le persone con le quali l'utente è stato in stretto contatto durante il periodo epidemiologicamente rilevante ai fini del tracciamento dei contatti.
- Il funzionamento di questo tipo di applicazioni potrebbe richiedere, a seconda dell'architettura prescelta, l'utilizzo di un server centralizzato. In tal caso, conformemente ai principi della minimizzazione dei dati e della protezione dei dati fin dalla progettazione, i dati trattati dal server centralizzato dovrebbero limitarsi al minimo necessario:
  - Quando a un utente viene diagnosticata l'infezione, d'accordo con l'utente possono essere raccolte le informazioni relative ai precedenti contatti ravvicinati o gli identificativi trasmessi dall'app. Occorre stabilire un metodo di verifica che consenta di certificare che la persona è realmente infetta senza identificare l'utente. Tecnicamente ciò sarebbe possibile allertando i contatti solo dopo l'intervento di un operatore sanitario, ad esempio utilizzando un codice speciale monouso.
  - Le informazioni memorizzate nel server centrale non dovrebbero consentire al titolare del trattamento di identificare gli utenti con diagnosi di infezione né i soggetti che sono venuti in contatto con tali utenti, e neppure dovrebbero consentire di effettuare inferenze sulla rete di contatti se non per ciò che è necessario ai fini della determinazione dei contatti pertinenti.
- Il funzionamento di un'app di questo tipo richiede la trasmissione di dati che sono letti e ascoltati dai dispositivi di altri utenti:
  - È sufficiente lo scambio di identificativi pseudonimizzati tra i dispositivi mobili degli utenti (computer, tablet, orologi connessi, ecc.), ad esempio mediante loro trasmissione attraverso il Bluetooth a bassa energia.
  - Gli identificativi devono essere generati utilizzando i processi più avanzati di crittografia.
  - Gli identificativi devono essere rinnovati regolarmente per ridurre il rischio di tracciamento fisico e di attacchi diretti.
- Questo tipo di applicazione deve essere protetto in modo da garantire la sicurezza dei processi tecnici di elaborazione. In particolare:
  - L'app non dovrebbe fornire agli utenti informazioni che consentano loro di desumere l'identità o la diagnosi di soggetti terzi. Il server centrale non deve né identificare gli utenti né effettuare inferenze nei loro riguardi.

Avvertenza: I principi di cui sopra si riferiscono all'obiettivo dichiarato delle *app di tracciamento dei contatti*, e unicamente a tale obiettivo, ossia fornire in modo automatico informazioni ai soggetti potenzialmente esposti al virus (senza necessità di identificarli). I gestori delle app e delle relative infrastrutture sono soggetti alle verifiche delle competenti autorità di controllo. L'osservanza della totalità o di parte di questi orientamenti non è sufficiente di per sé a garantire la piena conformità al quadro normativo in materia di protezione dei dati.

2. DEFINIZIONI

Contatto	Con riguardo a una app di tracciamento dei contatti, un contatto è un utente che ha partecipato a un'interazione con un altro utente di cui è confermato lo stato di positività al virus, per un periodo e a una distanza tali da comportare un rischio di esposizione significativa all'infezione. I parametri relativi alla durata dell'esposizione e alla distanza interpersonale devono essere definiti dalle autorità sanitarie e possono essere configurati nella app.
Dati relativi all'ubicazione	Qualsiasi dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale di un utente di un servizio di comunicazione elettronica accessibile al pubblico (quale definito nella direttiva e-privacy), nonché i dati provenienti da altre fonti potenziali relativi a: • latitudine, longitudine o altitudine dell'apparecchiatura terminale; • la direzione di marcia dell'utente; o • l'ora in cui sono state registrate le informazioni relative all'ubicazione.
Interazione	Nel contesto di un'app di tracciamento dei contatti, per interazione si intende lo scambio di informazioni tra due dispositivi situati in prossimità reciproca (nello spazio e nel tempo), all'interno del range proprio della tecnologia di comunicazione utilizzata (ad esempio Bluetooth). Questa definizione esclude l'ubicazione dei due utenti partecipanti all'interazione.
Vettore del virus	In questo documento sono considerati vettori del virus gli utenti che sono risultati positivi al virus e che hanno ricevuto una diagnosi ufficiale da medici o centri sanitari.

Tracciamento dei contatti	Chi si è trovato a stretto contatto (secondo i criteri epidemiologici) con persone infette dal virus corre un rischio significativo di essere infetto e di infettare a sua volta altre persone. Il tracciamento dei contatti è una metodologia di controllo delle patologie che prevede la creazione di un elenco di tutte le persone che si sono trovate nelle immediate vicinanze di un vettore del virus, in modo da verificare se siano a rischio di infezione e adottare nei loro confronti misure sanitarie adeguate.

3. INDICAZIONI GENERALI

GEN-1	L'app deve essere uno strumento complementare alle tecniche convenzionali di tracciamento dei contatti (in particolare la raccolta dell'anamnesi di persone infette), ossia deve far parte di un programma di sanità pubblica più ampio. Deve essere utilizzata solo fino a quando le tecniche di tracciamento manuale dei contatti non consentiranno in modo autonomo di gestire il numero delle nuove infezioni.
GEN-2	Occorre prevedere una procedura per interrompere la raccolta degli identificativi (disattivazione generale dell'app, istruzioni per la disinstallazione dell'app, disinstallazione automatica, ecc.) e per la cancellazione di tutti i dati raccolti da tutte le banche dati (applicazioni mobili e server), da attivare al più tardi quando le autorità pubbliche competenti avranno stabilito che la situazione si è «normalizzata ».
GEN-3	Il codice sorgente dell'app e del suo back-end deve essere pubblicamente disponibile e le specifiche tecniche devono essere rese pubbliche, in modo che le parti interessate possano verificare il codice e, se del caso, contribuire a migliorarlo correggendo eventuali bug e garantendo la trasparenza nel trattamento dei dati personali.
GEN-4	Il processo di implementazione dell'app deve consentire di validarne progressivamente l'efficacia in termini di salute pubblica. A tal fine occorre definire previamente un protocollo di valutazione che specifichi gli indicatori utili a misurare l'efficacia dell'app.

4. FINALITÀ

PUR-1	L'app deve mirare unicamente al tracciamento dei contatti, in modo da avvertire e prendere in carico i soggetti potenzialmente esposti al SARS-CoV-2. Non deve essere utilizzata per altre finalità.
PUR-2	L'utilizzo dell'app non deve derogare dalla sua finalità primaria allo scopo di controllare la conformità alle misure di quarantena o di confinamento e/o di distanziamento sociale.
PUR-3	L'app non deve essere utilizzata per trarre conclusioni sull'ubicazione degli utenti in base alla loro interazione e/o ad altri elementi.

5. CONSIDERAZIONI FUNZIONALI

FUNC-1	L'app deve fornire una funzionalità che consenta agli utenti di essere informati di una loro potenziale esposizione al virus; tale informazione deve basarsi sulla prossimità a un utente infetto verificatasi entro un periodo di X giorni prima del test di screening positivo (dove il valore X è definito dalle autorità sanitarie).
FUNC-2	L'app dovrebbe fornire indicazioni agli utenti identificati come potenzialmente esposti al virus. Dovrebbe trasmettere istruzioni sulle misure da adottare e consentire all'utente di chiedere un consulto. In tal caso sarebbe obbligatorio un intervento umano.
FUNC-3	L'algoritmo che misura il rischio di infezione alla luce dei fattori distanza e tempo, e che quindi stabilisce quando inserire un contatto nell'elenco di tracciamento dei contatti, deve essere regolabile in modo sicuro per tener conto delle conoscenze più recenti sulla diffusione del virus.
FUNC-4	**Gli utenti devono essere informati di essere stati esposti al virus**, o devono ricevere periodicamente informazioni indicanti se siano stati esposti o meno al virus, durante il periodo di incubazione del virus stesso.

6. DATI

DATA-1	L'app deve essere in grado di trasmettere e ricevere dati attraverso tecnologie di comunicazione di prossimità quali il Bluetooth a bassa energia in modo da poter effettuare il tracciamento dei contatti.
DATA-2	I dati trasmessi devono comprendere identificativi pseudo-casuali, con chiave di cifratura forte, generati dall'app e specifici per quest'ultima.
DATA-3	Il rischio di collisione tra gli identificativi pseudo-casuali dovrebbe essere sufficientemente basso.
DATA-4	Gli identificativi pseudo-casuali devono essere rinnovati regolarmente, con una frequenza sufficiente a limitare il rischio di reidentificazione, tracciamento fisico o collegamento tra individui da parte di qualsiasi soggetto, compresi il gestore del server centrale, altri utilizzatori dell'app o terzi malintenzionati. Questi identificativi devono essere generati dall'app, eventualmente sulla base di un seme (seed) fornito dal server centrale.
DATA-5	In conformità al principio della minimizzazione dei dati, l'app non deve raccogliere dati diversi da quelli strettamente necessari ai fini del tracciamento dei contatti
DATA-6	L'app non deve raccogliere dati relativi all'ubicazione ai fini del tracciamento dei contatti. I dati relativi all'ubicazione possono essere trattati al solo scopo di consentire l'interazione con applicazioni simili in altri paesi e dovrebbero limitarsi a quelli strettamente necessari, in termini di precisione, per tale unico scopo.
DATA-7	L'app non dovrebbe raccogliere dati relativi alla salute ulteriori rispetto a quelli strettamente necessari ai fini dell'app stessa, tranne che su base facoltativa e al solo scopo di supportare il processo decisionale mirato all'informazione dell'utente.
DATA-8	Gli utenti devono essere informati di tutti i dati personali che saranno raccolti. Tali dati dovrebbero essere raccolti solo previa autorizzazione dell'utente.

7. CARATTERISTICHE TECNICHE

TECH-1	L'app dovrebbe utilizzare le tecnologie disponibili per individuare utenti in prossimità del dispositivo che abbiano installato l'applicazione, ad esempio tecnologie di comunicazione di prossimità (come il Bluetooth a bassa energia).
TECH-2	L'app dovrebbe conservare lo storico dei contatti di un utente all'interno del dispositivo, per un periodo limitato e predefinito.
TECH-3	L'app può utilizzare un server centralizzato per implementare alcune funzionalità.
TECH-4	L'architettura dell'app deve sfruttare per quanto possibile i dispositivi degli utenti.
TECH-5	La trasmissione al server centrale dello storico dei contatti o degli identificativi degli utenti dovrebbe avvenire su iniziativa degli utenti stessi che risultino infetti e previa conferma di tale status da parte di un professionista sanitario abilitato.

8. SICUREZZA

SEC-1	Occorre verificare lo status degli utenti segnalati nell'app come positivi al SARS-CoV-2, ad esempio fornendo un codice monouso legato a un laboratorio o a un operatore sanitario. Se non è possibile ottenere conferma in modo sicuro, i dati non devono essere trattati.
SEC-2	I dati inviati al server centrale devono essere trasmessi attraverso un canale sicuro. Dovrebbe essere attentamente valutato il ricorso ai servizi di notifica messi a disposizione dai fornitori di piattaforme OS, che non dovrebbero comportare la divulgazione di dati a terzi.
SEC-3	Le richieste non devono essere vulnerabili rispetto a manipolazioni da parte di utenti malintenzionati.

SEC-4	Devono essere implementate le tecniche più avanzate di crittografia per garantire la sicurezza degli scambi tra l'applicazione e il server e tra le singole applicazioni, nonché, in via generale, per proteggere le informazioni memorizzate nell'app e sul server. Tra gli esempi di tecniche utilizzabili figurano la cifratura simmetrica e asimmetrica, funzioni di hash, protocolli PMT (*private membership test*), protocolli PSI (*private set intersection*), filtri di Bloom, *private information retrieval*, cifratura omomorfica, ecc.
SEC-5	Il server centrale non deve conservare gli identificativi di connessione alla rete (ad es. indirizzi IP) degli utenti, compresi quelli che hanno ricevuto una diagnosi positiva e che hanno trasmesso la cronologia dei contatti o i propri identificativi.
SEC-6	Al fine di evitare sostituzioni di persona o la creazione di utenze inesistenti (*fake*), il server deve autenticare l'app.
SEC-7	L'app deve autenticare il server centrale.
SEC-8	Le funzionalità dei server dovrebbero essere protette da attacchi di replay.
SEC-9	Per autenticarne origine e integrità, le informazioni trasmesse dal server centrale devono essere firmate.
SEC-10	L'accesso ai dati conservati nel server centrale e non accessibili al pubblico deve essere limitato esclusivamente alle persone autorizzate.
SEC-11	Il *permission manager* del dispositivo a livello di sistema operativo deve chiedere esclusivamente le autorizzazioni necessarie per accedere a e utilizzare i moduli di comunicazione, ove necessario, per conservare i dati nel terminale e per scambiare informazioni con il server centrale.

9. PROTEZIONE DEI DATI PERSONALI E DELLA PRIVACY DELLE PERSONE FISICHE

Nota: le indicazioni fornite di seguito riguardano un'app il cui unico scopo è il tracciamento dei contatti.

PRIV-1	Gli scambi di dati devono rispettare la privacy degli utenti (in particolare garantire il rispetto del principio di minimizzazione).
PRIV-2	L'app non deve consentire l'identificazione diretta degli utenti.
PRIV-3	L'app non deve consentire il tracciamento degli spostamenti degli utenti.
PRIV-4	L'utilizzo dell'app non dovrebbe consentire agli utenti di acquisire informazioni su altri utenti (in particolare se siano vettori del virus o meno).
PRIV-5	Il margine di fiducia riservato al server centrale deve essere limitato. La gestione del server centrale deve seguire regole di governance chiaramente definite e comprendere tutte le misure necessarie per garantirne la sicurezza. La localizzazione del server centrale dovrebbe consentire una vigilanza efficace da parte dell'autorità di controllo competente.
PRIV-6	Deve essere effettuata una valutazione d'impatto sulla protezione dei dati le cui risultanze dovrebbero essere rese pubbliche.
PRIV-7	L'app dovrebbe informare l'utente solo dell'esposizione al virus e, se possibile, senza rivelare informazioni su altri utenti, del numero e delle date dei relativi eventi.
PRIV-8	Le informazioni trasmesse dall'app non devono consentire agli utenti di identificare gli utenti vettori del virus né i loro spostamenti.
PRIV-9	Le informazioni trasmesse dall'app non devono consentire alle autorità sanitarie di individuare utenti potenzialmente esposti senza il loro previo accordo.
PRIV-10	Le richieste inviate dall'app al server centrale non devono rivelare alcuna informazione sul vettore del virus.

PRIV-11	Le richieste inviate dall'app al server centrale non devono rivelare informazioni superflue sull'utente, con la sola eccezione, ove necessario, degli identificativi pseudonimizzati e dell'elenco dei contatti.
PRIV-12	Non devono essere possibili attacchi di *linkage*.
PRIV-13	Gli utenti devono essere in grado di esercitare i propri diritti attraverso l'app.
PRIV-14	La cancellazione dell'app deve comportare la cancellazione di tutti i dati raccolti localmente.
PRIV-15	L'app dovrebbe raccogliere esclusivamente dati trasmessi da altre istanze dell'app stessa, ovvero da altre app interoperabili di analoga natura. Non devono essere raccolti dati relativi ad altre applicazioni e/o dispositivi di comunicazione di prossimità.
PRIV-16	Al fine di evitare la re-identificazione da parte del server centrale, dovrebbero essere utilizzati server proxy. Attraverso questi *server indipendenti* è possibile combinare gli identificativi di più utenti (sia appartenenti a vettori del virus sia inviati da altri richiedenti) prima di condividerli con il server centrale, in modo da impedire a quest'ultimo di conoscere gli identificativi (ad esempio gli indirizzi IP) specifici dei singoli utenti.
PRIV-17	Sviluppo e configurazione di app e server devono essere condotti con la massima cura al fine di evitare la raccolta di dati non necessari (ad esempio, nei log del server non dovrebbero essere inclusi identificativi, ecc.) nonché per impedire il ricorso a pacchetti di sviluppo software di terzi che raccolgano dati per altri fini.

La maggior parte delle app di tracciamento dei contatti allo studio prevede sostanzialmente due approcci qualora un utente risulti infetto: possono inviare al server la cronologia dei contatti di prossimità ottenuti mediante scansione, oppure inviare l'elenco dei propri identificativi già trasmessi. I principi ricordati di seguito sono declinati in base a questi due approcci. Tuttavia, ciò non significa che non siano possibili o addirittura preferibili altri approcci, basati per esempio sull'implementazione di forme di cifratura *end-to-end* (E2E) o sull'utilizzo di altre tecnologie di sicurezza o di potenziamento della privacy.

9.1 PRINCIPI CHE SI APPLICANO SOLO SE L'APP INVIA AL SERVER UN ELENCO DI CONTATTI:

CON-1	Il server centrale deve raccogliere la cronologia dei contatti degli utenti che siano stati certificati positivi al SARS-CoV-2 soltanto quale effetto di una scelta volontaria della persona dichiarata infetta.
CON-2	Il server centrale non deve conservare né distribuire un elenco degli identificativi pseudonimizzati degli utenti che siano vettori del virus.
CON-3	La cronologia dei contatti memorizzati sul server centrale deve essere cancellata una volta che gli utenti abbiano ricevuto notifica della loro prossimità a una persona risultata positiva.
CON-4	Nessun dato deve lasciare il dispositivo dell'utente se non qualora un utente risultato positivo condivida la cronologia dei contatti con il server centrale ovvero qualora un utente presenti al server una richiesta di informazioni sulla sua esposizione potenziale al virus.
CON-5	Qualsiasi identificativo presente nella cronologia conservata in locale deve essere cancellato dopo X giorni dalla raccolta (il valore X è definito dalle autorità sanitarie).
CON-6	Le cronologie dei contatti inviate da utenti distinti non dovrebbero essere oggetto di trattamenti ulteriori, ad esempio mediante correlazioni incrociate miranti a realizzare mappe globali di prossimità.
CON-7	I dati nei log di server devono essere ridotti al minimo e soddisfare i requisiti in materia di protezione dei dati

9.2 PRINCIPI CHE SI APPLICANO SOLO SE L'APP INVIA AL SERVER UN ELENCO DEI PROPRI IDENTIFICATIVI:

ID-1	Il server centrale deve raccogliere gli identificativi trasmessi dall'app di utenti di cui sia stata accertata la positività al SARS-CoV-2, a seguito di un intervento volontario da parte di tali utenti.
ID-2	Il server centrale non deve conservare né diffondere la cronologia dei contatti di utenti che siano vettori del virus.
ID-3	Gli identificativi memorizzati nel server centrale devono essere cancellati una volta distribuiti alle altre applicazioni.
ID-4	Eccettuati i casi in cui l'utente risultato positivo condivida i propri identificativi con il server centrale, ovvero qualora un utente chieda al server informazioni sulla sua potenziale esposizione al virus, nessun dato deve lasciare il device dell'utente.
ID-5	I dati nei log di server devono essere ridotti al minimo e soddisfare i requisiti in materia di protezione dei dati.

NOTE

[1] I riferimenti agli "Stati membri" contenuti nel presente documento vanno intesi come riferimenti agli "Stati membri del SEE".

[2] Si veda la precedente dichiarazione del Comitato europeo per la protezione dei dati sul focolaio di COVID-19.

[3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpblletterecadvisecodiv-appguidancefines.pdf

[4] Cfr. articolo 2, lettera c), della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

[5] Cfr. articoli 6 e 9 della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

[6] La nozione di consenso nella direttiva relativa alla vita privata e alle comunicazioni elettroniche coincide con quella di cui al RGPD e deve soddisfare tutti i requisiti previsti dal consenso di cui all'articolo 4 (11) e all'articolo 7 del RGPD.

[7] Per l'interpretazione dell'articolo 15 della direttiva e-privacy, cfr. anche la sentenza della Corte di giustizia dell'Unione europea del 29 gennaio 2008 nella causa C-275/06, Productores de Musica de España (Promusicae) c. Telefonica de Espana SAU.

[8] Si veda la sezione 1.5.3 delle Linee guida 1/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi.

[9] (de Montjoye et al., 2018) "On the privacy-conscientious use of mobile phone data".

[10] (de Montjoye et al., 2013) "Unique in the Crowd: The privacy bounds of human mobility" e (Pyrgelis et al.,
2017) "Knock Knock, Who's There? Membership Inference on Aggregate Location Data".

[11] Vedi anche la comunicazione della Commissione "Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection" (Orientamenti sulle app per le azioni di sostegno alla lotta alla pandemia da COVID-19 in relazione alla protezione dei dati), Bruxelles, 16.4.2020, C (2020) 2523 final.

[12] Vedi Considerando (41).

[13] I titolari del trattamento (in particolare le autorità pubbliche) devono prestare particolare attenzione al fatto che il consenso non dovrebbe essere considerato liberamente espresso se la persona non ha l'effettiva possibilità di rifiutare o di revocare il proprio consenso senza subire pregiudizio.

[14] Il trattamento deve basarsi sul diritto dell'Unione o degli Stati membri che preveda misure appropriate e specifiche per tutelare i diritti e le libertà della persona interessata, in particolare il segreto professionale.

[15] Si veda l'articolo 9, paragrafo 2, lettera h), del Regolamento generale sulla protezione dei dati.

[16] Si vedano le Linee guida del WP29 (fatte proprie dal Comitato europeo per la protezione dei dati) sulla valutazione d'impatto sulla protezione dei dati e sulla circostanza per cui il trattamento "possa comportare un rischio elevato" ai fini del regolamento (UE) n. 2016/679.

[17] Si vedano le Linee guida del comitato europeo per la protezione dei dati 4/2019 sulla protezione dei dati fin dalla fase di progettazione e per impostazione predefinita.

[18] In via generale, la soluzione decentrata è maggiormente conforme al principio di minimizzazione.

Torna a **Indice** | **Premessa**

Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19.

Adottata il 19 marzo 2020

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI HA ADOTTATO LA SEGUENTE DICHIARAZIONE:

Governi e organismi pubblici e privati di tutta Europa stanno adottando misure per contenere e attenuare il COVID-19. Ciò può comportare il trattamento di diverse tipologie di dati personali.

Le norme in materia di protezione dei dati (come il regolamento generale sulla protezione dei dati) non ostacolano l'adozione di misure per il contrasto della pandemia di coronavirus. La lotta contro le malattie trasmissibili è un importante obiettivo condiviso da tutte le nazioni e, pertanto, dovrebbe essere sostenuta nel miglior modo possibile. È nell'interesse dell'umanità arginare la diffusione delle malattie e utilizzare tecniche moderne nella lotta contro i flagelli che colpiscono gran parte del mondo. Il Comitato europeo per la protezione dei dati desidera comunque sottolineare che, anche in questi momenti eccezionali, titolari e responsabili del trattamento devono garantire la protezione dei dati personali degli interessati. Occorre pertanto tenere conto di una serie di considerazioni per garantire la liceità del trattamento di dati personali e, in ogni caso, si deve ricordare che qualsiasi misura adottata in questo contesto deve rispettare i principi generali del diritto e non può essere irrevocabile. L'emergenza è una condizione giuridica che può legittimare limitazioni delle libertà, a condizione che tali limitazioni siano proporzionate e confinate al periodo di emergenza.

1. LICEITÀ DEL TRATTAMENTO

Il **regolamento generale sulla protezione dei dati (RGPD) è una normativa di ampia portata e contiene disposizioni che si applicano anche al trattamento dei dati personali in un contesto come quello relativo al COVID-19**. **Il RGPD consente alle competenti autorità sanitarie pubbliche e ai datori di lavoro di trattare dati personali nel contesto di un'epidemia, conformemente al diritto nazionale e alle condizioni ivi stabilite**. Ad esempio, se il trattamento è necessario per motivi di interesse pubblico rilevante nel settore della sanità pubblica. In tali circostanze, non è necessario basarsi sul consenso dei singoli.

1.1 Per quanto riguarda il trattamento dei dati personali, comprese le categorie particolari di dati, da parte di autorità pubbliche competenti (ad es. autorità sanitarie pubbliche), il Comitato ritiene che gli articoli 6 e 9 del RGPD consentano tale trattamento, in particolare quando esso ricada nell'ambito delle competenze che il diritto nazionale attribuisce a tale autorità pubblica e nel rispetto delle condizioni sancite dal RGPD.

1.2 Nel contesto lavorativo, il trattamento dei dati personali può essere necessario per adempiere un obbligo legale al quale è soggetto il datore di lavoro, per esempio in materia di salute e sicurezza sul luogo di lavoro o per il perseguimento di un interesse pubblico come il controllo delle malattie e altre minacce di natura sanitaria. Il RGPD prevede anche deroghe al divieto di trattamento di talune categorie particolari di dati personali, come i dati sanitari, se ciò è neces-

sario per motivi di interesse pubblico rilevante nel settore della sanità pubblica (articolo 9.2, lettera i), sulla base del diritto dell'Unione o nazionale, o laddove vi sia la necessità di proteggere gli interessi vitali dell'interessato (articolo 9.2.c), poiché il considerando 46 fa esplicito riferimento al controllo di un'epidemia.

1.3 Per quanto riguarda il trattamento dei dati delle telecomunicazioni, come i dati relativi all'ubicazione, devono essere rispettate anche le leggi nazionali di attuazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche (direttiva e-privacy). In linea di principio, i dati relativi all'ubicazione possono essere utilizzati dall'operatore solo se resi anonimi o con il consenso dei singoli. Tuttavia, l'articolo 15 della **direttiva e-privacy consente agli Stati membri di introdurre misure legislative per salvaguardare la sicurezza pubblica**. Tale legislazione eccezionale è possibile solo se costituisce una **misura necessaria, adeguata e proporzionata all'interno di una società democratica**. Tali misure devono essere conformi alla Carta dei diritti fondamentali e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Inoltre, esse sono **soggette al controllo giurisdizionale della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo**. In presenza di situazioni di emergenza, le misure in questione devono essere rigorosamente limitate alla durata dell'emergenza.

2. PRINCIPI FONDAMENTALI RELATIVI AL TRATTAMENTO DEI DATI PERSONALI

I dati personali necessari per conseguire gli obiettivi perseguiti dovrebbero essere trattati per finalità specifiche ed esplicite.

Inoltre, gli interessati dovrebbero ricevere informazioni trasparenti sulle attività di trattamento svolte e sulle loro caratteristiche principali, compreso il periodo di conservazione dei dati raccolti e le finalità del trattamento. Le informazioni dovrebbero essere facilmente accessibili e formulate in un linguaggio semplice e chiaro.

È importante adottare adeguate misure di sicurezza e riservatezza che garantiscano che i dati personali non siano divulgati a soggetti non autorizzati. Si dovrebbero documentare in misura adeguata le misure messe in campo per gestire l'attuale emergenza e il relativo processo decisionale.

3. USO DEI DATI DI LOCALIZZAZIONE DA DISPOSITIVI MOBILI

- **I governi degli Stati membri possono utilizzare i dati personali relativi ai telefoni cellulari dei singoli nell'intento di monitorare, contenere o attenuare la diffusione del COVID-19?**

In alcuni Stati membri i governi prevedono di utilizzare i dati di localizzazione da dispositivi mobili per monitorare, contenere o attenuare la diffusione del CO-

VID-19. Ciò implicherebbe, ad esempio, la possibilità di geolocalizzare le persone o di inviare messaggi di sanità pubblica ai soggetti che si trovano in una determinata area, via telefono o SMS. **Le autorità pubbliche dovrebbero innanzitutto cercare di trattare i dati relativi all'ubicazione in modo anonimo (ossia, trattare dati in forma aggregata e tale da non consentire la successiva re-identificazione delle persone), il che potrebbe permettere di generare analisi sulla concentrazione di dispositivi mobili in un determinato luogo ("cartografia")**.

Le norme in materia di protezione dei dati personali non si applicano ai dati che sono stati adeguatamente anonimizzati.

Quando non è possibile elaborare solo dati anonimi, la direttiva e-privacy consente agli Stati membri di introdurre misure legislative per salvaguardare la sicurezza pubblica (articolo 15).

Qualora siano introdotte misure che consentono il trattamento dei dati di localizzazione in forma non anonimizzata, lo Stato membro ha l'obbligo di predisporre **garanzie adeguate**, ad esempio fornendo agli utenti di servizi di comunicazione elettronica il **diritto a un ricorso giurisdizionale**.

Si applica anche il principio di proporzionalità. Si dovrebbero sempre privilegiare le soluzioni meno intrusive, tenuto conto dell'obiettivo specifico da raggiungere. Misure invasive come il "tracciamento" (ossia il trattamento di dati storici di localizzazione in forma non anonimizzata) possono essere considerate proporzionate in circostanze eccezionali e in funzione delle modalità concrete del trattamento. Tuttavia, tali misure dovrebbero essere soggette a un controllo rafforzato e a garanzie più stringenti per assicurare il rispetto dei principi in materia di protezione dei dati (proporzionalità della misura in termini di durata e portata, ridotta conservazione dei dati, rispetto del principio di limitazione della finalità).

4. CONTESTO LAVORATIVO

- **Un datore di lavoro può chiedere ai visitatori o ai dipendenti di fornire informazioni sanitarie specifiche nel contesto del COVID-19?**

Nel caso di specie, è particolarmente pertinente l'applicazione dei principi di proporzionalità e di minimizzazione dei dati. Il datore di lavoro dovrebbe chiedere informazioni sanitarie soltanto nella misura consentita dal diritto nazionale.

- **Il datore di lavoro è autorizzato a effettuare controlli medici sui dipendenti?**

La risposta dipende dalle leggi nazionali in materia di lavoro o di salute e sicurezza. I datori di lavoro dovrebbero accedere ai dati sanitari e trattarli solo se ciò sia previsto dalle rispettive norme nazionali.

- **Il datore di lavoro può informare colleghi o soggetti esterni del fatto che un dipendente è affetto dal COVID-19?**

I datori di lavoro dovrebbero informare il personale sui casi di COVID-19 e adottare misure di protezione, ma non dovrebbero comunicare più informazioni del necessario. Qualora occorra indicare il nome del dipendente o dei dipendenti che hanno contratto il virus (ad esempio, in un contesto di prevenzione) e il diritto nazionale lo consenta, i dipendenti interessati ne sono informati in anticipo tutelando la loro dignità e integrità.

- **Quali informazioni trattate nel contesto del COVID-19 possono essere ottenute dai datori di lavoro?**

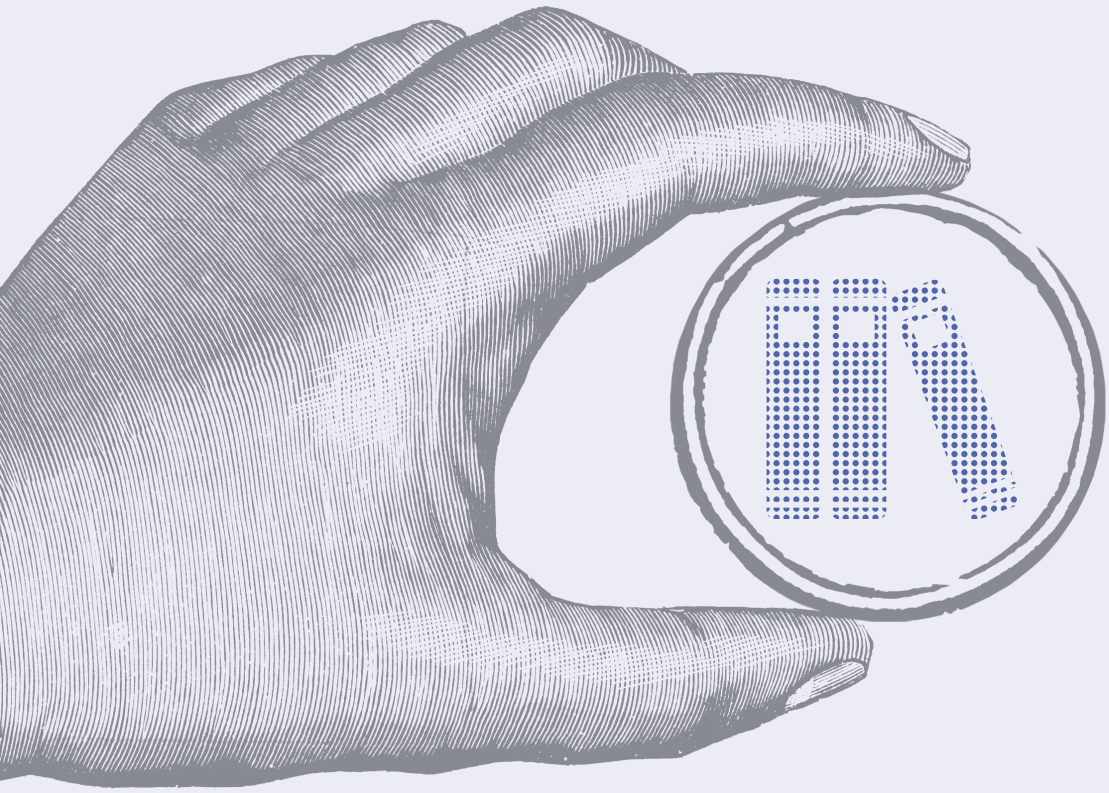
I datori di lavoro possono ottenere informazioni personali nella misura necessaria ad adempiere ai loro obblighi e a organizzare le attività lavorative, conformemente alla legislazione nazionale.

Per il Comitato europeo per la protezione dei dati
La presidente

(Andrea Jelinek)

Torna a **Indice**

6 Appendice



Riferimenti utili

- **EDPB**: Il Comitato europeo per la protezione dei dati (*European Data Protection Board*) è un organo europeo indipendente, istituito dal Regolamento europeo sulla protezione dei dati (GDPR), che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea (e nello Spazio Economico Europeo, SEE) e promuove la cooperazione tra le autorità competenti per la protezione dei dati. È composto da rappresentanti delle Autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati (EDPS). La Commissione europea e, per quanto riguarda le questioni connesse al regolamento generale sulla protezione dei dati, l'Autorità di vigilanza EFTA hanno titolo a partecipare alle attività e alle riunioni del comitato senza diritto di voto. Sostituisce il WP29. [https://edpb.europa.eu/]
- **EDPS/GEPD** - Garante europeo della protezione dei dati (*European Data Protection Supervisor*): L'Autorità di controllo indipendente incaricata di vigilare sul rispetto delle norme di protezione dei dati (fissate nel Regolamento (Ue) 2018/1725) da parte delle istituzioni, degli organi, delle agenzie e degli organismi dell'Unione europea. [https://edps.europa.eu/].
- **GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (GPDP)** – È l'Autorità indipendente di controllo incaricata in Italia dell'applicazione del GDPR/RGPD, ai sensi dell'art. 2-bis del decreto legislativo 196/2003. [http://www.garanteprivacy.it/]
- **WP29**: Il Gruppo di lavoro "Articolo 29" (*Article 29 Working Party*) era il gruppo di lavoro che riuniva le Autorità nazionali di vigilanza e protezione dei dati, all'interno dell'Unione europea. Era un organismo consultivo indipendente, composto da un rappresentante delle varie Autorità nazionali, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione. La sua istituzione e i compiti erano fissati nell'articolo 29 della direttiva europea 95/46, oggi abrogata. Dopo il 25 maggio 2018, è stato sostituito, con maggiori poteri e funzioni, dall'EDPB. [https://ec.europa.eu/newsroom/article29/items]

ALTRE ISTITUZIONI

- **CGUE / CURIA** - Corte di giustizia dell'Unione europea (Corte UE) [https://curia.europa.eu/]
- **DG JUST - Commissione europea** - Direzione generale giustizia e consumatori [https://ec.europa.eu/info/departments/justice-and-consumers_it]

DAL SITO DEL GARANTE:

- **GDPR/RGPD - Regolamento europeo in materia di protezione dei dati personali**: Pagina informativa completa [GDPR e Normativa europea e internazionale - Garante Privacy (gpdp.it)]
- **GDPR/RGPD – Guida sintetica** [Guida all'applicazione del GDPR - Garante Privacy (gpdp.it)]
- **GDPR/RGPD - Approfondimenti** [Approfondimenti GDPR - Garante Privacy (gpdp.it)]
- **Progetti formativi** [Progetti formativi - Garante Privacy (gpdp.it)]
  - **In particolare, materiali relativi ai progetti europei**:
    - ◊ T4DATA: Attività transnazionali di formazione e iniziative formative a livello nazionale dedicate ai Responsabili della Protezione dei Dati (RPD) operanti presso i soggetti pubblici.
    - ◊ SMEDATA: Strumenti pratici e interpretativi per supportare e formare i rappresentanti e gli esperti legali delle piccole e medie imprese (PMI) nell'applicazione e negli adempimenti del RGPD.
    - ◊ ARCII: Conoscenza e comprensione da parte delle PMI degli obblighi derivanti dal GDPR e dal quadro giuridico nazionale in materia di protezione dei dati personali; creazione di uno strumento digitale per la conformità al GDPR in formato *open source*.

A cura del
Servizio relazioni esterne e media

Per informazioni presso l'Autorità
Ufficio relazioni con il pubblico
lunedì - venerdì ore 10.00 - 12.30
tel. +39 06.69677.2917
e-mail: urp@gpdp.it

Edizione digitale Gennaio 2023

CONTRIBUTI

Le linee guida e gli altri documenti di lavoro approvati dai Garanti europei in seno all'EDPB

Questa seconda pubblicazione del Garante per la protezione dei dati personali raccoglie tutti i documenti riguardanti l'applicazione del GDPR, definitivamente approvati dal 2019 al 2022 dal Comitato europeo per la protezione dei dati (EDPB). Il volume offre chiarimenti e spunti di riflessione, in versione italiana, a tutti coloro che, per professione o per mero interesse personale, vogliano comprendere e tutelare diritti fondamentali – come quello alla privacy e alla protezione dati – che oggi rappresentano strumenti di democrazia, prima ancora che facilitatori dell'economia contemporanea.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI