Come adeguare la propria azienda al Regolamento Europeo sulla Privacy 679/2016

maggiolo pedini
associati

STUDIO MAGGIOLO PEDINI ASSOCIATI
Via Mons. Daniele Comboni, 3 | Padova 35136
T (direzione) 328.6241003 | T (amministrazione) 331.1880491
p. iva 03610290284 | SDI - KRRH6B9 | amministrazione@pec.studiomaggiolo.it
info@studiomaggiolo.it | www.studiomaggiolo.it |

ADEMPIMENTI OBBLIGATORI PER L'ADEGUAMENTO AL REGOLAMENTO UE 679/2016 (GDPR)

Ogni attività che effettua trattamento di dati di persone fisiche deve mettersi in regola: dalle grandi aziende alle medie imprese, alle piccole attività, compresi i liberi professionisti.

Tipologia trattamenti e categorie di interessati		Registro dei Trattamenti del Titolare (art. 30)	Registro dei Trattamenti del Responsabile (art. 30)	Informative clienti – fornitori (artt. 13-14)	Informative clienti con consenso (artt. 13-14)	Informative dipendenti (artt. 13-14)	Nomine dei responsabili esterni (art .28)	Procedura e Registro Data Breach (art. 33)	Formazione Titolare e autorizzati al trattamento (artt. 29-32-39)	Valutazione d'impatto D.P.I.A. (art. 35)	Gestione diritti interessati (artt. 15-16-17-18-19-21-22)	Adeguamento sito web (se presente)	Adeguamento portale e-commerce (se presente)
Dipendenti	SI	☑				☑	☑	☑	☑			☑	☑
	NO											☑	☑
Agenti commercio	SI	☑					☑	☑	☑			☑	☑
	NO											☑	☑
Clienti persone fisiche	SI	☑			☑		☑	☑	☑		☑	☑	☑
	NO											☑	☑
Clienti - fornitori Soggetti fiscali	SI	☑		☑			☑	☑	☑		☑	☑	☑
	NO											☑	☑
Attività di di marketing on-line e off-line	SI	☑		☑	☑		☑	☑	☑			☑	☑
	NO											☑	☑
Gestione fidelity card	SI	☑		☑	☑		☑	☑	☑	☑		☑	☑
	NO											☑	☑
Dati personali	SI	☑		☑	☑	☑	☑	☑	☑			☑	☑
	NO											☑	☑
Dati sulla salute	SI	☑		☑	☑	☑	☑	☑	☑	☑		☑	☑
	NO											☑	☑
Dati giudiziari	SI	☑		☑	☑	☑	☑	☑	☑	☑		☑	☑
	NO											☑	☑
Dati di minori	SI	☑		☑	☑		☑	☑	☑	☑		☑	☑
	NO											☑	☑
Trattamento dati conto terzi	SI	☑	☑	☑		☑	☑	☑	☑	☑		☑	☑
	NO											☑	☑

Cosa fare per essere in regola con il GDPR

In ogni azienda, a prescindere dalle dimensioni e dal settore merceologico, vengono trattati i dati personali dei clienti, dei dipendenti, dei fornitori e di tutte le persone che entrano in contatto con la realtà aziendale. Il regolamento UE 679/2016 (GDPR) prevede adempimenti specifici per chi effettua il trattamento dei dati personali, modulati diversamente in base al tipo ed alla quantità dei dati di cui si effettua il trattamento.

ADEMPIMENTO	RIFERIMENTO NORMATIVO
aggiornamento delle informative, diversificate per categorie di interessati (clienti – fornitori – dipendenti) e con specificazione della base giuridica del trattamento ed eventuale raccolta del consenso al trattamento	Articoli 12, 13 e 14 GDPR
verifica di conformità dei consensi raccolti prima del 25 maggio 2018 e predisposizione di nuovi moduli di raccolta per trattamenti successivi, con particolare riguardo al consenso dei minori	Articoli 7 e 8 GDPR e 2-*quinquies* D.lgs. 196/2003 s.m.i.
tenuta e aggiornamento del **Registro dei trattamenti** (titolare e responsabile)	Articolo 30 GDPR
nomina formale dei responsabili del trattamento, mediante contratto o altro atto giuridico che regoli i rapporti con il titolare e gli eventuali sub-responsabili	Articolo 28 GDPR e 2-*quaterdecies* del D.lgs. 196/2003 s.m.i.
verifica sull'eventuale contitolarità del trattamento tra più titolari	Articolo 26 GDPR
effettuazione di una valutazione di impatto nei casi di obbligatorietà e tracciabilità delle attività svolte, della mappatura dei rischi e delle misure adottate	Articoli 35 e 36 GDPR
regolarizzazione dei trasferimenti dei dati extra UE mediante le condizioni di legittimità previste dal GDPR	Articoli 44, 45, 46, 47 e 49 GDPR
piano per la gestione tempestiva dei *data breach* e dell'eventuale notificazione al Garante e/o comunicazione agli interessati	Articoli 32, 33 e 34 GDPR
piano per il riscontro tempestivo agli interessati in caso di esercizio dei diritti a loro spettanti	Articoli 15, 16, 17, 18, 19, 20, 21 e 22 GDPR
nomina del DPO (Data Protection Officer), nei casi di obbligatorietà e comunicazione dei dati al Garante	Articoli 37, 38 e 39 GDPR

I dati da tutelare

La classificazione dei dati secondo il GDPR:

- **dati personali che permettono l'identificazione diretta della persona -** ad esempio: nome e cognome, indirizzo, telefono, indirizzo e-mail, foto, video, etc;
- **dati che permettono l'identificazione indiretta della persona -** ad esempio: codice fiscale, indirizzo IP, numero di targa, etc;
- **dati genetici -** relativi alle caratteristiche genetiche ereditarie o acquisite
- **dati biometrici -** ottenuti da un trattamento tecnico relativo alle caratteristiche fisiche, fisiologiche o comportamentali
- **dati personali rientranti in particolari categorie -** ad esempio: quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale e quelli relativi all'orientamento sessuale;
- **dati relativi alla salute -** ad esempio: certificati medici, certificati idoneità al lavoro e/o alla attività sportiva, allergie a prodotti e/o ad alimenti, intolleranze ad alimenti, patologie invalidanti, anamnesi personale e/o familiare, reperti radiologici, etc;
- **dati riconducibili a minori;**
- **dati relativi a condanne penali e reati**.

Le sanzioni amministrative e penali

Sanzioni amministrative fino a 10 milioni di euro art. 83, comma 4	**Violazioni di minore gravità:** – Gli obblighi sanciti per il trattamento dei dati personali riguardanti soggetti minori di 16 anni (art. 8); – Gli obblighi previsti per il trattamento di dati senza necessaria identificazione dell'interessato (art. 11); – Gli obblighi relativi alla protezione dei dati personali fin dalla progettazione e per impostazione predefinita (ovvero il rispetto dei principi di privacy by design e privacy by default), alla tenuta dei registri delle attività di trattamento, alla cooperazione con l'autorità di controllo, nonché quelli previsti in materia di sicurezza del trattamento dei dati, di notifica delle violazioni dei dati all'autorità di controllo e all'interessato, così come gli obblighi riguardanti la valutazione d'impatto sulla protezione dei dati e la designazione del responsabile della protezione dei dati (artt. da 25 a 39); – Gli obblighi relativi ai meccanismi di certificazione della protezione dei dati (artt. 42 e 43).
Sanzioni amministrative fino a 20 milioni di euro art. 83, comma 5	**Violazioni di maggiore gravità:** – In base all'art. 5, i principi di correttezza, liceità e trasparenza del trattamento, il principio di limitazione della finalità del trattamento, il principio di minimizzazione, di esattezza, di limitazione della conservazione, di integrità e riservatezza dei dati personali e, infine, di responsabilizzazione del titolare del trattamento; – Il principio di liceità del trattamento dei dati espresso dall'art. 6, in forza del quale un trattamento sarà lecito se fondato sul consenso dell'interessato, se necessario per l'esecuzione di un contratto o di misure precontrattuali di cui l'interessato sia parte, o ancora per adempiere ad un obbligo di legge da parte del titolare del trattamento o per la tutela di interessi vitali dell'interessato o di un soggetto terzo, come per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, oppure per il perseguimento del legittimo interesse del titolare del trattamento o di terzi; – I principi che, in base all'art. 7, assicurano che la prestazione del consenso, da parte dell'interessato, al trattamento dei dati personali possa essere considerato legittimo; e infine – I principi a fondamento del legittimo trattamento di categorie particolari di dati personali, quali dati sensibili e dati relativi a condanne penali, come previsto dall'art. 9. – Diritti sanciti in capo ai soggetti interessati a norma degli artt. da 12 a 22 del GDPR, quali: – Il diritto di ricevere adeguate informazioni in ordine al trattamento dei propri dati personali (artt. da 12 a 14); – Il diritto di accesso (art. 15); – Il diritto di rettifica (art. 16); – Il diritto all'oblio (art. 17); – Il diritto alla limitazione del trattamento dei dati (art. 18); – Il diritto alla portabilità dei dati (art. 20); – Il diritto di opposizione al trattamento (art. 21); e, infine

	– Il diritto di non essere sottoposto a una decisione fondata unicamente su di un trattamento automatizzato, compresa la profilazione, e produttiva di effetti giuridici a suo carico (art. 22). – Disposizioni riguardanti il trasferimento di dati personali a un destinatario situato in un paese terzo o un'organizzazione internazionale (in base agli artt. da 44 a 49); – Obblighi sanciti dagli ordinamenti giuridici dei singoli stati membri e aventi ad oggetto specifiche situazioni di trattamento dei dati, come previsto ai sensi degli artt. da 85 a 91; e infine – Ordini o limitazioni provvisorie o definitive di trattamento stabilite dall'autorità di controllo, come previsto dall'art. 58, paragrafo 2.
Sanzioni penali	**Le fattispecie per cui sono applicabili sanzioni penali ai sensi del riformato Codice Privacy (D. Lgs. 101/2018):** – art. 167 (Trattamento illecito dei dati) – art. 167-bis (Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala); – art. 167-ter (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala); – art. 168 (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante); – art. 170 (Inosservanza dei provvedimenti del Garante).