

Il 25 Maggio 2018 è entrato in vigore il nuovo Regolamento Europeo per il trattamento dei dati personali.

Il GDPR (General Data Protection Regulation) disciplina la protezione dei dati personali nell'UE.

Alcune cose da sapere:

L'INFORMATIVA



Si tratta delle informazioni destinate all'interessato. Illustra in modo chiaro e sintetico i suoi obblighi e diritti e gli scopi e le modalità del trattamento. Deve essere chiara, semplice e facilmente accessibile e deve avere una forma concisa, trasparente, intelligibile. Viene consegnata per iscritto o in formato elettronico.

COSA SONO I DATI PERSONALI?

I dati personali sono quelle informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, relazioni personali, abitudini, stile di vita e situazione economica, ecc.



E I DATI PERSONALI PARTICOLARI?

Sono quei dati personali che rientrano in particolari categorie e sono definiti «*dati sensibili*», cioè che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, politiche, l'appartenenza sindacale, relativi alla salute, alla vita, all'orientamento sessuale e i dati genetici e biometrici.

COSA SI INTENDE PER TRATTAMENTO DEI DATI PERSONALI?



S'intende l'operazione o l'insieme di operazioni applicate ai dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la modifica, l'estrazione, la consultazione, l'utilizzo, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati.

PERCHÉ SI PARLA DI CONSENSO?



Per consenso si intende qualsiasi manifestazione di volontà libera, specifica, informata, preventiva e inequivocabile dell'interessato con cui egli manifesta il proprio assenso, mediante dichiarazione o azione positiva, che i suoi dati personali siano oggetto di trattamento. Non deve essere necessariamente documentato per iscritto o avere forma scritta e può essere implicito ma NON tacito o presunto (come nel caso di caselle pre-spuntate sui moduli). Nel caso invece di dati sensibili o processi decisionali automatizzati occorre un consenso esplicito.

COSA SIGNIFICA IL TERMINE ACCOUNTABILITY?

Indica la responsabilizzazione di Titolari e Responsabili del trattamento nell'adottare comportamenti proattivi tali da dimostrare l'adozione di misure concrete per assicurare l'applicazione del GDPR.



E L'ESPRESSIONE "PRIVACY BY DESIGN E BY DEFAULT"?

È il principio che implica la predisposizione di misure preventive volte alla protezione dei dati basandosi non solo su modelli standard (privacy by default), ma anche su procedure specifiche per la propria realtà (privacy by design) da parte del Titolare del trattamento.

CHI È L'INTERESSATO?



L'interessato è la persona fisica identificata o identificabile cui si riferiscono i dati personali.

CHI È LA FIGURA DEL DPO?



Il Data Protection Officer (Responsabile della protezione dei dati) è la figura che valuta e organizza la gestione del trattamento dei dati personali nel rispetto delle normative privacy. Ha inoltre la funzione di intermediario tra il Garante e l'interessato. Le amministrazioni, gli enti pubblici, i soggetti la cui attività principale consiste in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala e i soggetti la cui attività principale consiste nel trattamento su larga scala di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari o biometrici; hanno l'obbligo di nominare un DPO.

COS'È IL REGISTRO DEI TRATTAMENTI?

Si tratta del documento interno che contiene tutte le informazioni relative al trattamento, esiste in duplice copia (per il Titolare e per il Responsabile del trattamento).



CHI È IL TITOLARE DEL TRATTAMENTO?



È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che determina le finalità e i mezzi del trattamento.

CHI È 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.



CHE RUOLO HA IL DESTINATARIO?



Si tratta della 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).

COSA SI INTENDE PER DATA BREACH?



Si parla di data breach quando vi è una violazione di sicurezza nella quale i dati sensibili vengono consultati, copiati, trasmessi, rubati, persi, distrutti o utilizzati da un soggetto non autorizzato. In caso di violazioni, queste ultime devono essere segnalate al Garante e all'interessato entro 72 ore dalla violazione stessa.



A QUALI SANZIONI SI PUÒ ANDARE INCONTRO?

L'inosservanza delle disposizioni in tema di privacy può portare a sanzioni sino a un massimo di euro 20.000.000,00 o al 4% del fatturato mondiale totale annuo dell'esercizio precedente.



Garante per la protezione dei dati personali: www.garanteprivacy.it

