Privacy: Regolamento UE per il trattamento dei dati personali (GDPR 679/2016)

IL 25 maggio prossimo diventerà pienamente applicabile il Regolamento UE per il trattamento dei dati personali (GDPR 679/2016) in tutti i Paesi dell'Unione Europea e, in Italia, sostituirà le disposizioni del Codice della Privacy (D. lgs. 196/2003).

L'obiettivo del Regolamento è: protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali e alla relativa libertà di circolazione (art. 1).

Cosa sono i dati personali?

Qualsiasi informazione riguardante una persona fisica identificata o identificabile (art. 4, c. 1)

Il principio alla base della riforma è quello della "responsabilizzazione" secondo cui l'azienda o l'ente, denominati "titolari del trattamento" potranno liberamente valutare come conformarsi alla norma, ma dovranno rispondere della correttezza del loro operato.

COSA CAMBIA

Il consenso

Per i dati sensibili (ai sensi dell'art. 9) e per i trattamenti automatizzati, compresa la profilazione (art. 22) il consenso **deve essere esplicito.**

Il consenso non deve essere fornito per iscritto, anche se la forma scritta sia l'unica a garantirne l'inequivocabilità; il titolare, comunque, deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

Il consenso deve essere, in ogni caso, libero, specifico, informato e inequivocabile; **non è ammesso** il consenso tacito o presunto.

L'informativa

Qualora i dati personali siano raccolti presso l'interessato, il titolare del trattamento deve fornire specifiche informazioni **(c.d. obbligo di informativa).**

I contenuti dell'informativa sono elencati all'art. 13, in specifico:

- il titolare deve sempre specificare i dati di contatto del responsabile della protezione dei dati;
- la finalità del trattamento e la base giuridica del trattamento;
- il legittimo interesse del titolare o di terzi;
- gli eventuali destinatari dei dati personali;
- ove applicabile, l'intenzione del titolare di trasferire i dati personali a un Paese Terzo e attraverso quali strumenti.

Il Regolamento prevede, inoltre, ulteriori informazioni al fine di garantire un trattamento corretto e trasparente, quali il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione da parte del titolare e il diritto di presentare un reclamo all'autorità di controllo.

Nel caso in cui il trattamento comporti processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Qualora i dati non siano stati raccolti direttamente presso l'interessato (art. 14), l'informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese dalla raccolta**, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato).

L'informativa dovrà essere **concisa, trasparente, intellegibile** per l'interessato e **facilmente accessibile**; il linguaggio dovrà essere chiaro e semplice.

L'informativa è data **per iscritto** e preferibilmente in formato elettronico, anche se sono ammessi "altri mezzi", pertanto anche oralmente, nel rispetto delle caratteristiche specificate all'art. 12, paragrafo 1.

Il diritto di accesso (art. 15)

L'interessato ha diritto di ottenere l'accesso ai propri dati personali e alle relative informazioni e di ottenere una copia dei dati oggetto di trattamento.

Fra le informazioni che il titolare deve fornire non rientrano le modalità del trattamento, mentre è necessario indicare il periodo di conservazione previsto o, se non possibile, i criteri utilizzati per definire tale periodo e le garanzie applicate in caso di trasferimento dei dati verso Paesi Terzi.

Il Registro dei trattamenti (art. 30)

I titolari e i responsabili di trattamento, ad eccezione degli organismi con meno di 250 dipendenti, ma solo se non effettuano trattamenti a rischio (art. 30, paragrafo 5), hanno l'obbligo di tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

La tenuta del registro dei trattamenti non costituisce un adempimento formale, ma parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro.

Infatti, il registro è uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto/ente indispensabile per ogni valutazione e analisi del rischio.

Le misure di sicurezza

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1). Si specifica che la lista prevista dall'art. 32, paragrafo 1, è una lista aperta e non esaustiva. Pertanto, a partire dal 25 maggio, giorno di applicabilità diretta del Regolamento in tutti gli Stati membri, non potranno sussistere obblighi generalizzati di adozione di misure "minime" di sicurezza poiché la valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati.