PRIVACY E DPO

GDPR – REGOLAMENTO EUROPEO PRIVACY

Il Regolamento Europeo Privacy è entrato in vigore il 25 maggio 2016 e si applica in tutti gli Stati Membri dal 25 maggio 2018, termine ultimo per l'adeguamento alla nuova **legge sulla privacy.**

La versione definitiva del testo del GDPR 679/16 è stata pubblicata sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016. Il Regolamento fa riferimento alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

In Italia ha abrogato la direttiva 95/46/CE, così detta "Direttiva Madre" e ha sostituito il Codice Privacy.

Un po' di storia

Dopo un'evoluzione normativa durata decenni, la disciplina della protezione dei dati personali ha trovato un nuovo fondamento nel Regolamento Europeo Privacy, entrato in vigore il 25 maggio 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio dello stesso anno.

Tale "Regolamento UE 2016/679 Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", comunemente noto come GDPR o Regolamento Europeo Privacy, mira a creare un sistema di regole comuni che tuteli gli interessati rispetto agli effetti distorsivi della libera circolazione dei dati personali.

L'Unione Europea ha quindi fissato al 25 maggio 2018 il termine ultimo entro il quale gli Stati Membri hanno dovuto adeguarsi al GDPR. Per farlo, in Italia si è proceduto, attraverso il D.Lgs. 101/2018, ad armonizzare il preesistente Codice Privacy (il D. Lgs. 196/2003) con il nuovo testo del Regolamento Europeo.
È nata così una nuova normativa privacy nazionale, che prevede quindi la sopravvivenza del vecchio Codice Privacy, revisionato nel 2018 per allinearsi alla disciplina europea.

Regolamento Europeo Privacy e nuovi diritti

Il GDPR o Regolamento Europea Privacy ha introdotto nuove tutele a favore degli interessati, e inevitabilmente nuovi obblighi a carico di Titolari e Responsabili del trattamento di dati personali. Segnaliamo l'introduzione del diritto dell'interessato alla "portabilità del dato" (ad. es. nel caso in cui si intendesse trasferire i propri dati da un social network ad un altro) e del diritto all'oblio per cui ogni individuo può richiedere la cancellazione dei propri dati in possesso di terzi (per motivazioni legittime). Questo

"Il nostro ruolo è quello di aiutare le aziende ad avere successo nel mutevole panorama della privacy "

può accadere ad esempio in ambito web quando un utente richiede l'eliminazione dei propri dati in possesso di un social network o di altro servizio web.

Per Titolari e Responsabili del trattamento le novità sono state parecchie. **Il principio della accountability comporta l'onere di dimostrare l'adozione, senza convenzionalismi, di tutte le misure privacy adottate nel rispetto del Regolamento Europeo**. Bisogna redigere e conservare opportune documentazioni come il Registro delle attività di trattamento (art. 30) in cui vengano riportare tutte le attività di trattamento dati svolte sotto la responsabilità del titolare al trattamento o del responsabile. Viene richiesto di cooperare con l'autorità di controllo notificando qualsiasi violazione dei dati personali alla stessa e al diretto interessato (art. 32-34).

Il principio di accountability e i suoi strumenti

Un elemento fondamentale introdotto proprio dal GDPR è il cosiddetto "***principio di accountability"*, ossia di responsabilizzazione del titolare del trattamento,** che assume una duplice valenza: da un lato il dovere di adottare misure utili a prevenire i rischi per gli interessati, e dall'altro l'onere di documentare, anche in chiave probatoria, tutto ciò che viene fatto in relazione al trattamento di dati personali.

Posta l'importanza del principio di accountability, il titolare del trattamento dispone di una serie di strumenti che ne garantiscono la "responsabilizzazione", tra cui:

- Il Registro delle attività di trattamento ex art. 30 del GDPR, cioè un documento che permette di mappare le attività svolte raccogliendo al suo interno una descrizione di tutti i trattamenti di dati personali realizzati dal titolare e/o dal responsabile del trattamento.
- I principi di privacy by design e by default ex art. 25 del GDPR. Da un lato, la privacy by design prevede che venga garantita la protezione dei dati fin dalla progettazione dei trattamenti, mettendo in atto una serie di garanzie volte a tutelare gli interessati. Dall'altro lato, la privacy by default si riferisce alla protezione dei dati per impostazione predefinita, prevedendo che siano trattati solo i dati necessari alle finalità perseguite, escludendo ab origine le tipologie di trattamento considerabili superflue o ultronee rispetto agli scopi del titolare.
- La Valutazione di impatto sul trattamento dei dati ex art. 35 del GDPR, anche detta DPIA (Data Protection Impact Assessment), che prevede, sulla base di un risk-based approach, la valutazione dei rischi relativi ai trattamenti di dati personali svolti.

"Come è assicurato il livello di sicurezza dei dati ?"

"Quali sono gli strumenti di tutela ?"

L'attenzione alla protezione dei dati e all'approccio risk-based promossi dal Regolamento Europeo Privacy, sono ulteriormente ribadite dall'art. 32 del GDPR, che prevede una serie di misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio. Tali misure dovranno essere in grado, in particolare, di garantire "la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" (art. 32 par. 1 lett. b) del GDPR). La tutela dei cosiddetti Requisiti RID – Riservatezza, Integrità e Disponibilità – ai quali si associa anche il concetto di Resilienza, è infatti fondamentale per qualsiasi organizzazione che si trova a gestire delle informazioni, siano esse dati

personali o meno.

Alcune novità ulteriori del GDPR

All’interno delle altre novità previste dal Regolamento Europeo Privacy vi sono una serie di tutele a favore degli interessati, tra le quali si segnala **il diritto dell’interessato alla portabilità del dato**, cioè a ricevere i dati personali che lo riguardano e che questi siano trasmessi ad un altro titolare del trattamento (ad. es. nel caso in cui si intendesse trasferire i propri dati da un social network ad un altro). Oppure il **diritto all’oblio**, per cui ogni individuo può richiedere la cancellazione dei propri dati in possesso di terzi (per motivazioni legittime), come può accadere ad esempio in ambito web quando un utente richiede l’eliminazione dei propri dati in possesso di un social network o di altro servizio web.

O ancora **il diritto alla correzione dei dati,** sancito dall'art. 16 del Regolamento Europeo, che consente all'interessato di poter chiedere e ottenere dal titolare del trattamento la correzione dei propri dati, nel caso in cui questi risultano essere inesatti o incompleti.

Infine, un’altra novità fondamentale introdotta dal GDPR è il Responsabile della protezione dati o Data Protection Officer (DPO), una figura obbligatoria, con compiti di consiglio, informazione e controllo in merito agli obblighi relativi alla Privacy.

Chiedi al nostro Team per saperne di più in merito alla nomina del DPO e alla tutela dei dati personali.