



GDPR

Il **25 Maggio 2018** entrerà in vigore il nuovo regolamento UE in materia di data privacy, applicabile in tutti gli Stati membri dell'Unione Europea, senza che sia necessaria alcuna normativa interna di adeguamento.

In estrema sintesi, il GDPR – General Data Protection Regulation – obbliga le aziende ad assumersi maggiori responsabilità sui dati degli utenti raccolti e a impegnarsi per proteggerli al meglio.

L'intento principale del legislatore europeo è di creare un unico regime di protezione dei dati, che interessi tutti i soggetti che svolgono affari sul suolo europeo, compresi quelli che hanno ufficialmente sede fuori dall'Unione.

QUALI SONO LE PRINCIPALI NOVITÀ?

[Informativa e consenso](#)

Con l'attuale disciplina il testo con cui si informa l'utente circa le finalità e le modalità del trattamento dei dati personali è più che altro un documento burocratico, pieno di riferimenti legislativi. L'effetto è



Consulenza Gare - SOA - ISO



che l'utente viene disincentivato alla lettura e, di conseguenza, viene meno l'informazione stessa.

Il **GDPR** impone alle aziende di rendere l'informativa sulla privacy più comunicativa, affinché sia accessibile e comprensibile a chiunque.

Per quanto riguarda il consenso al trattamento dei dati, il nuovo Regolamento Ue prevede che questo possa essere manifestato dagli utenti in due modalità: in modo esplicito o attraverso azioni positive. Queste novità favoriranno le aziende nella raccolta dei dati, che saranno rilasciati in maniera più consapevole dalle persone interessate.

Profilazione

Il **GDPR** offre, finalmente, una definizione dell'attività di profilazione. L'art. 4 del Regolamento indica la profilazione come qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo degli stessi per valutare determinati aspetti relativi a una persona fisica. In particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le



preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti degli utenti.

Le aziende che intendono fare profilazione devono specificarlo nell'informativa e in tal caso è richiesto un consenso rafforzato, ossia esplicito. Non sarà quindi sufficiente il consenso per azioni positive.

DPO – Data Protection Officer

Il **GDPR** ha introdotto una nuova figura, il Responsabile della Protezione dei Dati. Si tratta di un supervisore interno che funge da collegamento tra l'azienda e l'Autorità Garante nazionale. Il DPO dovrà possedere un'adeguata conoscenza della normativa relativa alla gestione dei dati personali, dovrà adempiere alle sue funzioni in assenza di conflitti di interesse e potrà operare alle dipendenze del titolare oppure sulla base di un contratto di servizio.

Sanzioni

Le aziende che non si adegueranno alla normativa europea saranno soggette a sanzioni amministrative pecuniarie. Ad esempio, se un'azienda non segnala una violazione dei dati personali entro 72 ore, dovrà pagare una sanzione.



implementation: attuazione delle misure necessarie per mitigare i rischi rilevati (di conformità, preventive, correttive, tecnologiche e di formazione)

operations & support: gestione operativa dei dati (trattamento), dei diritti dell'interessato e dei data breach

2. Costruzione ed implementazione del sistema privacy GDPR consistente in:

Registro del trattamento dati strumento introdotto dal Regolamento Europeo per consentire alle autorità di controllo competenti di monitorare le attività di trattamento dei dati personali effettuate dal Titolare o dal Responsabile del trattamento sotto la propria responsabilità.

Regolamento sull'uso dei dati documento ad uso interno per tutto il personale nel quale viene dettagliata la metodologia circa l'uso dei dati gestiti dall'organizzazione

Procedura gestione incidente informatico procedura (step by step) da applicare in caso di incidente informatico

Registro incidenti informatici documento su cui annotare tutti gli eventuali incidenti informatici avvenuti all'interno dell'organizzazione

Informativa privacy aggiornamento dell'informativa presente sulla modulistica aziendale

Formazione al nuovo GDPR ad erogazione ultimata è prevista una specifica attività formativa ai soggetti coinvolti nella gestione dei dati (Titolare de dati e Responsabile del trattamento)

