Forse avete già sentito parlare del GDPR e magari sapete anche della sua prossima entrata in vigore il 25 maggio 2018: in caso contrario questo documento vuole essere una piccola introduzione sull'argomento.

**GDPR, chi era costui?**

GDPR è la sigla di "General Data Protection Regulation", ovvero il Regolamento dell'Unione Europea n. 679/2016 che riguarda la sicurezza dei dati personali di tutti i cittadini dell'Unione, che entrato in vigore il 24 maggio 2016 e diventerà pienamente operativo il 25 maggio 2018.
L'Unione si è data questo nuovo regolamento per armonizzare le norme di protezione della privacy dei singoli stati membri ("Un continente, una legge") e fornire norme certe ed uguali per tutte le istituzioni, le organizzazioni e le imprese che operano all'interno dell'UE, utilizzando dati personali dei cittadini europei, anche se hanno sede al di fuori dell'Unione (come ad esempio i giganti del web e dei social networks). Per quanto riguarda l'Italia il GDPR va quindi a sostituire completamente le precedenti norme del Codice della Privacy risalenti al 2004.
Il Regolamento introduce norme più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti e stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'UEe e per i casi di violazione dei dati personali ("data breach").

**Le novità del GDPR**

Il GDPR rovescia completamente la prospettiva della disciplina di riferimento, istituendo un quadro normativo tutto incentrato sui doveri e la responsabilizzazione del Titolare del trattamento (già presente nella nostra normativa), il cosiddetto principio di "accountability". La nuova disciplina impone a tale soggetto di garantire il rispetto dei principi in essa contenuti, ma anche di essere in grado di comprovarlo, adottando una serie di strumenti che lo stesso GDPR indica. La nuova normativa europea abbandona il concetto di "misure minime" del nostro Codice della Privacy, sostituendolo con quello di "misure adeguate". Questa maggiore discrezionalità, tuttavia, è accompagnata dall'onere attribuito al Titolare del trattamento di dimostrare le ragioni che hanno portato a una determinata decisione.

Accanto alla figura del Titolare del trattamento il GDPR inserisce la nuova figura del Data Protection Officer (DPO), ovvero uno specialista qualificato che supporti l'applicazione degli obblighi della nuova normativa e funga da punto di contatto con le Autorità di controllo e gli interessati. IL DPO è una figura particolare: deve essere indipendente e autonomo rispetto al Titolare, non ci deve essere conflitto di interessi con altre funzioni a lui affidate, non è rimosso o penalizzato dal titolare del trattamento per l'adempimento dei propri compiti. Il DPO deve godere di indipendenza ed autonomia di risorse per assolvere i compiti di protezione a lui affidati e mantenere la propria conoscenza specialistica al passo con le evoluzioni della tecnologia e dei rischi. La designazione del DPO è obbligatoria solo in alcuni casi (trattamenti dati su larga scala, trattamenti effettuati da un'Autorità pubblica, o trattamenti di categorie particolari di dati personali), tuttavia la presenza di un DPO costituisce una buona prassi anche per le aziende che sarebbero esenti da tale adempimento.

Una novità del GDPR è il concetto di "privacy by design", ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche. In quest'ottica si colloca l'obbligo per le aziende con più di 250 dipendenti o che trattano dati tali da presentare un rischio per i diritti e le libertà dell'interessato di tenere un "registro dei trattamenti" in formato cartaceo

o elettronico. La tenuta del registro costituisce un adempimento di fondamentale importanza per il principio di accountability, in quanto permette di monitorare in maniera approfondita le operazioni di trattamento all'interno dell'organizzazione. Esso costituisce dunque sia uno strumento operativo di lavoro con cui censire in maniera ordinata le banche dati e gli altri elementi rilevanti per assicurare un sano "ciclo di gestione" dei dati personali, sia un vero e proprio documento di carattere probatorio mediante il quale il Titolare del trattamento può dimostrare di aver adempiuto alle prescrizioni del Regolamento.

**Un po' di nomenclatura e qualche collegamento**

| | |
|---|---|
| Dati personali | Qualsiasi informazione riguardante una persona fisica identificata o identificabile; ad esempio il nome, un codice di identificazione, dati relativi all'ubicazione geografica, un identificativo online, uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica |
| Trattamento | Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione |
| Violazione dei dati personali | Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati |
| Dati genetici | Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione |
| Dati biometrici | Dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici |

Innanzitutto si consulti la pagina principale del Garante della Privacy sul nuovo regolamento europeo:
http://www.garanteprivacy.it/regolamentoue
Importante è anche la guida del Garante all'applicazione del regolamento:
http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali
E per finire ecco il collegamento ai testi ufficiali del Regolamento e della Direttiva UE:
http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT
http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L0680&from=IT