GDPR

A partire dal 25 maggio 2018 è direttamente applicabile in tutti gli Stati membri il **Regolamento Ue 2016/679**, noto come **GDPR** (General Data Protection Regulation) – relativo alla protezione delle persone fisiche con riguardo al **trattamento e alla libera circolazione dei dati personali**.

In sintesi col GDPR:

- Si introducono regole più chiare su informativa e consenso;
- Vengono definiti i limiti al trattamento automatizzato dei dati personali;
- Poste le basi per l'esercizio di nuovi diritti;
- Stabiliti criteri rigorosi per il trasferimento degli stessi al di fuori dell'Ue;
- Fissate norme rigorose per i **casi di violazione dei dati** (**data breach**).

Le priorità operative sono tre:

- La designazione in tempi stretti del Responsabile della protezione dei dati;
- L'istituzione del Registro delle attività di trattamento;
- La notifica dei data breach.

Il principio di "responsabilizzazione"

E' stata introdotta la **responsabilizzazione dei titolari del trattamento** (accountability) e un approccio che tenga in maggior considerazione i **rischi** che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

Data breach Gdpr

Il **titolare del trattamento dovrà comunicare eventuali violazioni** dei dati personali al Garante. **Rispondere in modo efficace a un data breach per il Gdpr**

Il primo adempimento da porre in essere per le imprese italiane è senz'altro l'adozione del **Registro dei trattamenti di dati personali.** Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone:

- Il titolare **dovrà informare** in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare i danni;
- Potrà decidere di **non informare** gli interessati se riterrà che la violazione non comporti un rischio elevato per i loro diritti oppure se dimostrerà di avere già adottato misure di sicurezza; oppure, infine, nell'eventualità in cui informare gli interessati potrebbe comportare uno sforzo sproporzionato al rischio.
- **L'Autorità Garante** potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria valutazione dei rischi correlati alla violazione commessa.

Le responsabilità e le sanzioni per le aziende

Ci sono diverse fattispecie e si va da un mera diffida amministrativa a sanzioni fino a 20 milioni di euro.

La figura del DPO (Data Protection Officer)

Non a caso è stata prevista la figura del "**Responsabile della protezione dei dati" (Data ProtectionOfficer o DPO)**, **incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti** e individuato in funzione delle qualità professionali e della conoscenza specialistica della normativa e della prassi in materia di protezione dati.

Il Responsabile della protezione dei dati:

1. Riferisce direttamente al vertice,
2. E'indipendente, non riceve istruzioni per quanto riguarda l'esecuzione dei compiti;
3. Gli vengono attribuzione risorse umane e finanziarie adeguate alla mission.

Il DPO deve avere una specifica competenza "della normativa e delle prassi in materia di dati personali nonché delle norme e delle procedure amministrative che caratterizzano il settore".

I poteri dell'autorità di controllo (Garante privacy)

All'autorità di controllo, il nostro Garante Privacy, sono conferiti poteri di indagine, correttivi, autorizzativi e consultivi, oltre al potere di infliggere sanzioni amministrative pecuniarie.

DPIA
Data Protection Impact assessment

Il DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.
Non è obbligatoria se non quando un trattamento può presentare un rischio elevato per i diritti e le libertà personali.
Comunque sia, la **raccolta dei dati aziendali**, non costa molto in termini di tempo ed è sicuramente una buona pratica per valutare e dimostrare la conformità ai principi del GDPR.

La **raccolta** di **informazioni** è la prima cosa da fare.

Misura di sicurezza fisica/organizzativa degli edifici
Misure di sicurezza fisica/organizzativa del CED
Asset presenti e relativo livello di criticità

Rilevamento archivi:

- cartacei
- magnetici/ottici
- altro tipo
- contenuto
- livello riservatezza

misure sicurezza

Rilevazione del S.I (hw, sw,archivii elettronici)

hardware (pc,server, host, ecc.)
software installato
archivi presenti
servizi erogati
criteri di manutenzione