Protezione dei dati e GDPR

Adeguarsi al GDPR - Regolamento (UE) 2016/679

1) Chi deve adeguarsi?

Qualsiasi organizzazione, associazione, azienda, scuola etc. (con sede in uno dei paesi dell'Unione Europea) pubblica o privata che si trova a **gestire dati personali** è **tenuta per legge a rispettare le norme del GDPR.**

2) Censire e mappare itrattamenti

La mappatura dei flussi di dati e la raccolta della documentazione interna riguardante il trattamento dei dati personali è un passo necessario per misurare concretamente l'impatto del Regolamento sull'attività della propria impresa, nonché per ottenere un'adeguata consapevolezza sulla sicurezza dei dati trattati.
Questa fase è importante anche per una corretta impostazione del Registro delle attività di trattamento ("Registro"), nuovo adempimento previsto dall'art. 30 del GDPR, per identificare quei trattamenti a rischio elevato che richiederanno una apposita valutazione dell'impatto sulla protezione dei dati.
Per ogni trattamento dei dati personali sarà dunque necessario domandarsi quanto segue:

Chi determina le finalità e i mezzi dei trattamenti effettuati? Ovvero chi effettua concretamente l'attività trattamento dei dati (incaricato, Responsabile, sub-Responsabile).
Quali categorie di dati vengono trattati; Quali rischi comporta il trattamento di ciascuna categoria di dati identificati.
Perché i dati sono raccolti | elaborati | divulgati | conservati | cancellati o distrutti.
Dove i dati in questione vengono custoditi e trattati; Dove gli stessi potranno venire trasferiti.
Quando i dati vengono raccolti.
Come viene garantita la protezione dei dati personali e quali misure di sicurezza sono poste in essere per ridurre al minimo i rischi di accesso non autorizzato ai dati.

Approfondimenti

*Il Regolamento ha previsto che il **Titolare del trattamento** sarà **direttamente responsabile** per le violazioni della normativa, introducendo anche un obbligo di **responsabilità solidale in capo al Responsabile del trattamento**. Il GDPR specifica dettagliatamente le caratteristiche dell'atto con cui viene designato il Responsabile: dovrà trattarsi di un **contratto**, o di un altro atto giuridico conforme al diritto interno, che indichi tassativamente tutte le informazioni necessarie per dimostrare il rispetto delle istruzioni impartite dal Titolare, nonché delle disposizioni del Regolamento stesso.*

Il Responsabile potrà a sua volta nominare un sub-Responsabile del trattamento, per lo svolgimento di specifiche attività, nel rispetto degli stessi obblighi contrattuali intercorrenti fra il Titolare e il Responsabile primario; quest'ultimo risponderà davanti al primo dell'eventuale inadempimento del sub-Responsabile.

3) Analizzare i rischi e individuare le priorità

Durante la fase di mappatura dei trattamenti, sarà necessario identificare i principali rischi a cui è esposta l'azienda ed individuare le azioni da intraprendere per risultare adempienti al Regolamento. È utile in questa fase verificare che:

- siano stati raccolti solo i dati strettamente necessari per il raggiungimento delle finalità perseguite;
- sussista una base giuridica per il trattamento, quali, *inter alia*, il consenso dell'interessato, il legittimo interesse del Titolare, la sussistenza di un rapporto contrattuale con l'interessato, una disposizione di legge specifica, etc.;
- siano in vigore le misure di sicurezza adeguate;
- siano garantiti i diritti degli interessati, come ad esempio: diritto di accesso, rettifica, diritto alla portabilità, revoca del consenso;
- siano rispettate tutte le disposizioni in tema di sicurezza, privacy e protezione dei dati personali.

4) Un'impostazione di vigilanza speciale sarà richiesta in caso di:

- trattamento di **particolari categorie di dati** (i.e. dati che rivelino la presunta origine razziale o etnica, opinioni politiche, filosofiche o religiose, appartenenza sindacale; lo stato di salute o l'orientamento sessuale dell'interessato; dati giudiziari; dati relativi ai minori);
- trasferimento dei dati al di fuori dall'Ue;
- specifiche finalità di trattamento (i.e. monitoraggio sistematico su larga scala di un'area accessibile a livello pubblico; monitoraggio su larga scala di dati di categorie particolari e dati giudiziari; profilazione o altre attività sistemiche sulla base delle quali vengono prese decisioni che hanno effetti giuridici sulle persone fisiche).

In questi casi il trattamento potrebbe richiedere un'attività preventiva a tutela dell'interessato.

I nuovi diritti in gioco

*> Il GDPR rafforza i diritti degli interessati e la protezione dei dati personali. In particolare, agevola gli interessati nell'**accedere** alle informazioni riguardanti i propri dati personali e conoscere come questi vengano processati, gestiti ed eventualmente trasferiti all'estero dai Titolari e Responsabili del Trattamento.*

Il nuovo ventaglio di diritti in capo agli interessati del trattamento comprende anche:

- *il **diritto all'oblio** (art. 17 GDPR), ovvero il diritto ad ottenere la cancellazione dei propri dati personali qualora essi non risultino più necessari rispetto alle finalità perseguite dal Titolare del trattamento;*
- *il **diritto di sapere quando i propri dati siano stati violati** (c.d. "Data breach");*
- *il **diritto di opporsi al marketing diretto** (art 21.3 GDPR);*

***il diritto alla portabilità dei dati**, ossia a ricevere dal Titolare i propri dati, su un supporto informatico leggibile, per trasmetterli senza alcun impedimento da parte del Titolare stesso ad un diverso Titolare del trattamento.*

5) Designare il Data Protection Officer

Tra le innovazioni più rilevanti nella struttura organizzativa disegnata dal GDPR vi è **la nomina del Data Protection Officer (DPO)**, ovvero del soggetto che assume all'interno dell'impresa una funzione di informazione, consulenza e controllo della gestione del trattamento di dati.

Il DPO dovrà essere una persona "*che abbia conoscenza della normativa e delle pratiche in materia di protezione di dati nel controllo del rispetto del Regolamento*", come indica l'art. 97 del GDPR.

Per assistere le imprese nell'esecuzione degli obblighi imposti dalla normativa in materia di protezione dei dati personali, il DPO dovrà:

- conoscere approfonditamente il GDPR e le altre disposizioni normative applicabili in materia di privacy;
- porre in essere azioni di sensibilizzazione sull'impatto dei trattamenti operati dall'impresa;
- monitorare ed indirizzare costantemente la conformità al GDPR.

6) I processi interni

Al fine di garantire un adeguato livello di protezione dei dati personali risulta necessario **aggiornare e implementare** i processi organizzativi interni all'impresa.

Tale fase non potrà prescindere dalla considerazione di quegli eventi che possono incidere sul trattamento, come ad esempio i data breach, la conservazione dei dati raccolti o l'esercizio da parte degli interessati dei propri diritti.

L'organizzazione dei processi interni impone alle aziende di:

- implementare misure tecniche ed organizzative secondo i principi" By Default" e "By Design";
- prevedere piani di formazione dei dipendenti;
- gestire in modo efficiente i reclami e le richieste degli interessati, nonché garantire l'esercizio dei loro diritti alla cancellazione e/o di accesso, rettifica, opposizione, portabilità e revoca del consenso;
- notificare le violazioni dei dati all'Autorità competente entro 72 ore e, ove necessario, agli interessati.

Il DPO

Il GDPR ha previsto la designazione obbligatoria del DPO nei casi in cui il trattamento dei dati:

- *avvenga da parte di un'autorità od organismo pubblico*
- ***consista nel monitoraggio regolare e sistematico dei dati degli interessati, su larga scala,***
- *riguardi, sempre su larga scala, dati personali di speciali categorie, come ad esempio quelli sensibili o giudiziari. Tuttavia, all'infuori di queste ipotesi, la nomina di un DPO è comunque consigliabile al fine di garantire la comprensione degli obblighi del Regolamento, il rispetto della normativa ed il dialogo con le Autorità di protezione dei dati, nonché ovviamente per ridurre al minimo i rischi di una controversia.*

7) Gestire i rischi

L'adozione e corretta tenuta del Registro dei trattamenti da parte di tutti i soggetti attivi del trattamento, ancorché non obbligatoria ai sensi dell'art. 30 del GDPR, consente di censire e conservare con precisione tutti gli elementi rilevanti per assicurare un sano "ciclo di gestione" del dato personale e dei rischi ad esso connessi.

Inoltre, qualora un particolare trattamento presenti un elevato rischio per i diritti e le libertà dei soggetti interessati, il Titolare è tenuto a svolgere anche la DPIA.

Ma concretamente, cosa contiene una DPIA?

- La descrizione del trattamento e delle finalità perseguite;
- la valutazione delle necessità e della proporzionalità del trattamento;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- l'indicazione delle misure previste per risolvere tali rischi e dunque conformarsi al Regolamento, tra cui:
  - ridurre al minimo i dati raccolti e consentire l'esercizio dei diritti;
  - eseguire il back up dei dati, tracciare ogni tipo di attività, gestire prontamente la violazione dei dati;
- controllare l'accesso ai dati e la gestione;
- ridurre la vulnerabilità di hardware, software, reti e documenti.

8) Documentare la conformità

Il corretto processo di adeguamento al GDPR si conclude con la redazione di documenti di rendicontazione delle attività svolte, in cui venga presentato in modo sistematico e funzionale il piano di rimedi elaborati e di quelli da implementare per contrastare i profili di rischio emersi, e segnatamente:

- **Registro di trattamento** (da aggiornare periodicamente in base alle finalità ed al tipo di trattamento svolto dall'impresa);
- DPIA (da ripetere ogni tre anni).

Inoltre, il Titolare ed il Responsabile sono tenuti a dimostrare documentalmente di aver:

- **reso idonea informativa all'interessato**;
- raccolto, ove necessario, il consenso libero specifico, informato ed inequivocabile al trattamento;
- **provveduto a designare i Responsabili** (o sub-Responsabili) del trattamento mediante contratto o altro atto giuridico idoneo a tale scopo;
- **posto in essere qualsiasi altro adempimento** o attività richiesto dal Regolamento (i.e. l'ottemperamento ad una legittima richiesta dell'interessato; nomina del DPO; etc.).

Privacy by Design e by Default

*Quali misure di attuazione del principio di accountability, il Titolare pone in essere comportamenti che consentano la concreta attuazione dei principi di protezione dei dati direttamente dalla **fase di ideazione e progettazione del trattamento**.*

Ulteriore fil rouge nella gestione del trattamento rispetto al principio di accountability, è l'onere di mettere in atto misure tali per cui il trattamento di dati personali avvenga, per impostazione predefinita, solo se strettamente necessario per le finalità perseguite dallo stesso.

Sanzioni

Il GDPR prevede, in caso di violazione, ingenti sanzioni amministrative pecuniarie che possono giungere, fino a 20.000.000,00 di euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

In particolare, l'infrazione delle prescrizioni che regolano la tenuta del Registro l'esecuzione della PIA può comportare l'irrogazione di una sanzione amministrativa fino a 10.000.000,00 di euro, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83.4.a. GDPR).

Soltanto un efficiente sistema di gestione della privacy consentirà di evitare le ingenti sanzioni riducendo gli imprevisti a minor rischio.

Quali servizi di consulenza possiamo offrirvi:

- Assistenza nell'adeguamento al Regolamento europeo 2016/679 ivi compreso il servizio DPO.
- La mappatura dei flussi di dati e la raccolta e revisione della documentazione interna;
- Supporto nella redazione e/o nell'implementazione del Registro dei Trattamenti;
- Supporto nella redazione della documentazione (informative, disciplinare sull'utilizzo di strumenti informatici, nomine ad incaricati e responsabili, nomine Ads, ed ogni documento utile)
- Analisi dei rischi e consulenza per l'adozione delle misure minime di sicurezza previste ed *audit*;
- Notifica all'Autorità Garante e supporto nell'applicazione dei provvedimenti dell'autorità stessa;
- Assistenza annuale e supporto nelle procedure di verifica necessarie tra cui quella dei responsabili nominati;
- Assistenza sulle varie tematiche inerenti alla Data Protection tra cui:
  - Videosorveglianza
  - Cloud
  - Siti web
  - App
  - Marketing
  - trattamento dati del personale
  - amministratori di sistema