REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

nuovi obblighi e adempimenti in materia di privacy con scadenza 25 maggio 2018

docente avv. Giovanni Dal Poz

STUDIO LEGALE DAL POZ & PARTNERS

copernico CENTRO STUDI

Per maggiori info scrivere a comunicazione@copernicocs.it oppure chiamare lo 0422/306792

www.copernicocs.it

Regolamento europeo in materia di protezione dei dati personali

Che cos'è il GDPR?

Il Regolamento Generale sulla Protezione dei Dati è la nuova normativa europea che armonizza e supera le normative attualmente vigenti negli Stati facenti parte della Comunità Europea, punta a rafforzare e proteggere da minacce presenti e future i diritti alla protezione dei dati sensibili dei propri cittadini, dentro e fuori dall'Unione Europea.

Per farlo, il GDPR introduce nuovi obblighi e nuove sanzioni che impongono alle aziende l'adozione di specifiche misure per la protezione dei dati personali.

Regolamento europeo in materia di protezione dei dati personali

Questo impone alle aziende l'urgenza di indirizzare correttamente i propri investimenti verso adeguati strumenti informatici e procedurali al fine di ridurre il rischio di pesanti sanzioni pecuniarie ed integrarli alle nuove polizze assicurative per la copertura degli eventuali danni propri e a terzi.

Tra gli elementi introdotti dalla normativa si sono:

Regolamento europeo in materia di protezione dei dati personali

- la necessità gestire un registro dei trattamenti e garantire nel tempo la sicurezza dei dati;

- l'obbligo di notificare i data breach (ossia, un incidente di sicurezza in cui dati sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato);

Regolamento europeo in materia di protezione dei dati personali

- l'esigenza di introdurre la figura dell' RPD o DPO (Data Protection Officer);

- l'esigenza di adottare un approccio ispirato al principio di "Privacy by Design" (con cui si intende il principio di incorporazione della privacy a partire dalla progettazione di un processo aziendale con le relative applicazioni informatiche di supporto).

Regolamento europeo in materia di protezione dei dati personali

La principale differenza rispetto al passato è che gestire la "privacy" all'interno dell'organizzazione non potrà più essere un semplice adempimento, a volte più formale che sostanziale, ai singoli obblighi normativi, ma bensì implicherà l'impostazione di un processo che prevede l'analisi dei rischi e la gestione nel tempo, con continuità e nel fermo rispetto dei diritti di ogni individuo, dei dati personali trattati in ogni singola realtà aziendale.

Regolamento europeo in materia di protezione dei dati personali

Quali sono le attività da fare per adeguarsi al GDPR?

Le attività fondamentali per preparare la tua azienda a fronteggiare il cambiamento sono:

- comprendere come i nuovi obblighi previsti dalla normativa europea impatteranno sulle attività quotidiane;
- determinare quali sono e dove si trovano i dati sensibili e come sono messi in sicurezza;

Regolamento europeo in materia di protezione dei dati personali

- nominare un Data Protection Officer, dove necessario (una figura professionale con particolari competenze in campo informatico, giuridico, di valutazione del rischio e di analisi dei processi, il cui compito principale sarà l'osservazione, la valutazione e la gestione del trattamento dei dati personali allo scopo di far rispettare le normative europee e nazionali in materia di privacy);
- rivedere tutte le normative sulla privacy;
- rivedere i processi di accesso ai dati, rettifica e cancellazione richieste dalle persone interessate.

Regolamento europeo in materia di protezione dei dati personali

CONSAPEVOLEZZA: E' opportuno conoscere tutte le vulnerabilità dell'azienda, avviando un'indagine approfondita di tutti i sistemi interni e/o esterni per avere piena consapevolezza delle fragilità e dei rischi a cui si è esposti, in modo da proteggere i dati ed agevolare il processo di conformità.

Regolamento europeo in materia di protezione dei dati personali

MAPPATURA DEI DATI: Necessaria per analizzare la portabilità dei dati, i diritti di accesso a cancellazione. Per creare una buona mappatura è necessario scoprire e classificare i dati personali, le prime informazioni da proteggere. La conoscenza è alla base di GDPR, "Non puoi proteggere ciò che non conosci".

Regolamento europeo in materia di protezione dei dati personali

Cosa si intende per "Dati Personali" (Personal Data)?

I dati personali sono tutte quelle informazioni che si riferiscono ad un persona identificata o identificabile.

Cosa si intende per identificabile?

E' la persona fisica che può essere individuata direttamente o indirettamente. In quest'ultimo caso, non si considera quindi "Dato Personale" solamente un'informazione univoca di un individuo (nome, email, codice fiscale, ecc.) ma anche un insieme di dati generici, che se non correlati tra loro possono ricondurre ad uno specifico individuo.

Regolamento europeo in materia di protezione dei dati personali

MONITORAGGIO: E' fondamentale considerare il diritto delle persone di tracciare i dati di accesso, modificarli, cancellarli o trasferirli. Gli individui possono richiedere alle organizzazioni che possiedono dati sul loro conto, il diritto di rettificare, cancellare o trasferire dati. Il regolatore dovrebbe essere obbligato a rispondere alle richieste della persona, senza indebito ritardo ed al più tardi entro un mese.

Regolamento europeo in materia di protezione dei dati personali

Perché è importante? Le multe più alte di GDPR sono proprio per la violazione dei diritti della persona interessata, come per la mancata risposta o la fornitura di informazioni adeguate. L'interessato ha inoltre il diritto al risarcimento monetario dei danni.

Le aziende hanno quindi bisogno di strumenti per dimostrare che le richieste vengono processate in modo tempestivo.

Regolamento europeo in materia di protezione dei dati personali

SICUREZZA: La messa in sicurezza dei dati personali non potrà più essere presa alla leggera! Rispetto alla normativa italiana prevista dal Garante della Privacy, il testo europeo innalza significativamente il livello di protezione dei dati richiesto.

"Occorre attuare misure tecniche ed organizzative per garantire un livello di sicurezza adeguato".

Regolamento europeo in materia di protezione dei dati personali

Cosa si intende?

Il testo pone l'attenzione sui "rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati."

Regolamento europeo in materia di protezione dei dati personali

Tra le misure contemplate dalla norma approvata dalla Comunità Europea troviamo:

la pseudonimizzazione e la cifratura dei dati personali;

la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative per garantire la sicurezza del trattamento.

Regolamento europeo in materia di protezione dei dati personali

NOTIFICA: Sarà importante segnalare le violazioni in modo tempestivo. Nel caso di una violazione dei dati personali, il responsabile del trattamento, senza indebito ritardo (entro e non oltre 72 ore dopo l'avvenimento) deve comunicare tale violazione all'autorità di vigilanza.

Regolamento europeo in materia di protezione dei dati personali

Come previsto dall'articolo 33, la comunicazione al Garante dovrà contenere:

la descrizione della violazione;

la natura dei dati interessati;

la probabili conseguenze della violazione;

le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e/o per attenuare i possibili effetti negativi.

Regolamento europeo in materia di protezione dei dati personali

In sostanza "il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze ad essa relative, le sue conseguenze ed i provvedimenti adottati per porvi rimedio." Questa documentazione consentirà all'autorità garante di verificare il rispetto della norma da parte del titolare del trattamento dei dati.