General Data Protection Regulation

25 MAGGIO 2018

Il **Regolamento Generale per la Protezione dei Dati personali** n. 2016/679 (***General Data Protection Regulation*** o ***GDPR***) è la normativa di riforma della legislazione europea in materia di protezione dei dati 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.
Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, è entrato in vigore il 24 maggio 2016, ma la sua attuazione avverrà, però, a distanza di due anni, quindi dal **25 maggio 2018**.

A differenza della direttiva esistente dal 1995 sulla protezione dei dati, il GDPR creerà un quadro di legge armonizzato e unificato per tutti i paesi dll'UE.

Questo comporterà necessariamente una trasformazione nel modus operandi e nella mentalità degli addetti ai lavori rispetto alla governance delle informazioni aziendali. Alcuni spunti di riflessione rispetto alla nuova normativa:

- Obbligo di conformazione prodotti IT a normativa.
- Obbligo conformazione data center a normativa.
- Una sola regolamentazione per un solo continente - *proteggere i dati aziendali equivale a proteggere il business*.
- Notificazioni delle violazioni agli utenti interessati ed alle autorità nazionali nei casi di data breach.
- Diritto alla portabilità dei dati (anche rispetto all'incremento delle sempre più diffuse wearable technology).
- Normativa proporzionata al rischio.
- Privacy by design e by default.
- Rapporto con i fornitori che dovranno uniformarsi alla normativa, anche se allocati extra-UE.
- Responsabilità di Controller (Titolare) e Processor.
- DPO – Data Protection Officer.
- Nuovo sistema sanzionatorio. - fino a 20 milioni di euro o il 4% del fatturato
- Semplificazioni per le PMI.

Questo è il momento di costruire sulle fondamenta di cui disponi per garantirti protezione, controllo e conoscenza dei tuoi dati.

Il GDPR introduce nuovi obblighi e nuove sanzioni che impongono alle aziende l'adozione di specifiche misure per la 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 e integrarli alle nuove polizze assicurative per la copertura degli eventuali danni propri e a terzi.

C'è tempo fino al 25 maggio 2018, ma la portata innovativa del regolamento è imponente.
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. Implicherà l'impostazione di un processo, analizzare i rischi e gestire, nel tempo e con continuità i dati personali che si trattano (nel fermo rispetto dei diritti di ogni individuo).

La normativa prevede una multa fino a **20 milioni di euro o il 4% del fatturato** annuo globale per ogni caso di violazione nei seguenti casi:

- per chi non si adegua alla nuova normativa entro il termine previsto dalla Comunità Europea;
- nei casi in cui, nonostante l'adempimento, emergono carenze regolamentari a seguito di una violazione dei dati.

Le fasi del cambiamento

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

- Comprendere come i nuovi obblighi previsti da GDPR impatteranno sulle attività.
- Determinare quali sono e dove si trovano i dati oggetto del GDPR e come sono messi in sicurezza.
- Nominare un Data Protection Officer, dove necessario.
- Rivedere tutte le informative sulla privacy.
- Rivedere il processo di accesso ai dati, rettifica e cancellazione richieste dalle persone interessate.

Ecco i 5 punti da cui partire.

1 CONSAPEVOLEZZA

È 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 e agevolare il processo di conformità.

2 MAPPATURA DEI DATI

Necessaria per analizzare la portabilità dei dati, i diritti di accesso e cancellazione. Per creare una buona mappatura è necessario scoprire e classificare i dati personali, le prime informazioni da proteggere. La conoscenza dei dati è alla base di GDPR, "***You cannot protect what you don't know about***".

Cosa si intende per "Personal Data"?

Il dato personale rappresenta lo strumento tecnico-giuridico attraverso il quale i legislatori, nazionali e comunitari, tutelano l'insieme dei diritti collegati all'identità personale, quindi è un bene giuridico di secondo grado.

Dato personale è qualsiasi informazione concernente una persona fisica identificata o identificabile, anche indirettamente, oppure informazioni riguardanti una persona la cui identità è nota o può comunque essere accertata mediante informazioni suplementari.

3 MONITORAGGIO

È 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 i dati. "*Il regolatore dovrebbe essere obbligato a rispondere alle richieste della persona, senza indebito ritardo e al più tardi entro un mese*".

Perché è importante: Le multe più alte di GDPR sono per la violazione dei diritti della persona interessata, come per la mancata risposta o la fornitura di informazioni adeguate.

L'interessato ha inoltre diritto al risarcimento monetario dei danni.

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

4 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.
Per la norma approvata dalla Comunità Europea "*occorre attuare misure tecniche e organizzative per garantire un livello di sicurezza adeguato*".

Cosa si intende?

Il testo pone l'attenzione su "*i 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*".

Tra le misure di protezione contemplate dalla legge, si annovera:

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

Si introduce inoltre il principio di "Data Protection By Design" e "Privacy by Default", un approccio concettuale innovativo che impone alle aziende l'obbligo di avviare un progetto prevedendo, fin da subito, gli strumenti a tutela dei dati personali.

5 NOTIFICA

Sarà importante segnalare le violazioni in modo tempestivo. Nel caso 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.

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

- La descrizione della violazione
- La natura dei dati interessati
- Le probabili condseguenze 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.

In sostanza "*il titolare del trattamento, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e 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.

LA FILOSOFIA

Chi ha tempo non lo butti via, bensì lo utilizzi per governare al meglio il processo che conduce alla compilance e colga l'opportunità di adottare procedure e tecnologie che oltre a garantire il rispetto della normativa accrescano il livello di sicurezza e la continuità operativa.

3nd progetti può aiutarvi a riconoscere e gestire le informazioni che necessitano di una corretta Data Privacy e **capire lo stato di salute della Vostra infrastruttura informatica** tramite servizi di:

Gap Analysis	Indagine approfondita di tutti i sistemi interni e/o esterni per avere piena consapevolezza delle fragilità e dei rischi a cui si è esposti, con redazione di un documento in grado di evidenziare le vulnerabilità dell'azienda.
Vulnerability Assessment	Attività che consiste nell'identificare e correggere le vulnerabilità presenti sui sistemi prima che vengano messi in produzione oppure controllare con continuità quelle presenti su sistemi già rilasciati.
Penetration Testing	Metodo per valutare la sicurezza di un sistema o di una rete, l'analisi viene condotta simulando un'aggressione, al fine di individuare eventuali debolezze con particolare focus sugli accessi non autorizzati.

In qualità di ***Business Partner*** di SOPHOS (leader mondiale della sicurezza informatica), **3nd progetti** è in grado di fornire le migliori tecnologie sul mercato per raggiungere gli obiettivi oggetto del **GDPR**.