NUOVO REGOLAMENTO UE 2016/679 PRIVACY

Le novità introdotte dal nuovo regolamento UE 2016/679 in materia di protezione dei dati personali

Il General Data Protection Regulation (GDPR) andrà a sostituire le normative dei singoli Paesi Europei, diverse le une dalle altre. Costituisce un importante passo in avanti in tema di standardizzazione delle politiche europee e di protezione dei dati a livello continentale. L'estensione della giurisdizione del nuovo Regolamento Europeo sulla Protezione dei Dati Personali andrà a coinvolgere tutte le società che trattano dati personali di soggetti risiedenti nell'Unione Europea, indipendentemente dalla localizzazione geografica dell'azienda o del luogo in cui i dati vengono gestiti ed elaborati. Anche le imprese non europee che elaborano dati di cittadini europei dovranno comunque nominare un rappresentante interno all'UE.

IL GDPR DA MINACCIA AD OPPORTUNITÀ

Il 25 maggio 2018, data che segna l'entrata in vigore del Regolamento Europeo sulla Protezione dei Dati Personali (General Data Protection Regulation, GDPR), si sta avvicinando. Numerose aziende vivono con ansia questo cambiamento che segna una rivoluzione per tutti che dovranno obbligatoriamente adeguarsi alla nuova normativa entro le scadenze stabilite. Concentrarsi per raggiungere la piena conformità al GDPR è uno sforzo significativo per ogni azienda, specialmente per le piccole-medie imprese, ma che offre anche diverse opportunità per la crescita ed il business.

L'approccio stabilito è quello di basare la protezione dei dati sull'analisi del rischio, andando poi ad obbligare tutti coloro che hanno a che fare con la privacy di soggetti terzi all'introduzione di misure tecniche ed organizzative idonee al rischio emerso.

Il GDPR, inoltre, introduce sistemi di gestione per la privacy atti a dimostrare rapidamente e nella più totale trasparenza le procedure applicate fin dall'inizio del trattamento dei dati (privacy by design e by default). Questo passaggio risulta fondamentale per un'eventuale verifica da parte delle autorità di controllo e fornisce un valore aggiunto per la reputazione e l'immagine della compagnia. Un'impresa che applica in maniera adeguata il GDPR sarà infatti in grado di migliorare i legami verso la realtà con cui si interfaccia generando con la clientela un rapporto di reciproca fiducia. Un'azienda completamente compliance al GDPR dovrà sì investire per introdurre le misure richieste, ma potrà sfruttare quest'opportunità per trasformare il trattamento dei dati e la riservatezza in un suo punto di forza e non solo, sarà anche un vantaggio per l'organizzazione interna che avrà modo di mettere al sicuro dati sensibili e informazioni rilevanti ed essenziali del suo core business. In tale modo si può ottenere una maggior protezione sia per i dati relativi a terzi sia per sé stessi.

LE NOVITÀ INTRODOTTE DAL GDPR

Sono passati più vent'anni dalla direttiva 95/46/CE del Parlamento europeo e in questo lasso di tempo è avvenuta una totale rivoluzione tecnologica: nel 1995 internet non era presente in tutte le case, non esistevano "social network" e le tecnologie alla portata di tutti non erano assolutamente paragonabili a quelle di oggi. Si pensi solo agli smartphone, il primo è stato introdotto sul mercato dalla Apple nel 2007 con l'uscita dell'iPhone ed ora quasi ogni persona è in possesso di uno strumento simile che consente di restare connesso col mondo intero condividendo ed avendo accesso a dati, posizioni, fotografie e quant'altro con un semplice gesto del dito.

Alla luce di tutto ciò, si rese necessario apportare delle modifiche e di rinnovare le normative in tema di privacy. Il nuovo Regolamento Europeo sulla Protezione dei Dati Personali 679/2016 introduce alcune modifiche alla vecchia direttiva al fine di renderla più completa, facile da applicare e chiara per tutti coloro che desiderano accedere, modificare o cancellare i propri dati.

Le novità sono molte e le imprese dovranno predisporre di un piano di adeguamento ben definito per non farsi trovare impreparate il 25 maggio 2018.

Ecco le 10 novità che le aziende devono conoscere della nuova disciplina europea:

1. ***Inventario dei dati personali trattati dall'azienda***

Censimento dei dati personali, loro classificazione per tipologia (compresi web, social e APP) con relative responsabilità di trattamento

2. ***Conduzione analisi del rischio di trattamento improprio dei dati personali aziendali (Privacy Impact Assessment – PIA)***

- Definizione del campo di applicazione e della sua estensione
- Analisi del flusso dei dati correlati ai processi aziendali
- Analisi della Privacy tramite interviste e questionari
- Valutazione di probabilità e di impatto

3. ***Protezione dei dati fin dalla progettazione***

Le imprese titolari del trattamento dei dati dovranno:

- predisporre misure tecniche e organizzative interne adeguate a tutelare la privacy fin dalla progettazione di servizi e prodotti basati sul trattamento di dati personali [Privacy by Design];
- garantire che vengano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento [Privacy by Default];

4. ***Introduzione della figura del DPO (Data Protection Officer)***

Il DPO è una figura specifica all'interno dell'azienda che ha il compito fondamentale di fungere da tramite tra l'impresa e le autorità di controllo. È il responsabile della protezione dei dati col compito di valutare, sulla base dell'analisi dei rischi, se richiedere o meno un parere alle autorità di controllo.

5. ***Rafforzamento delle condizioni per la concessione del consenso***

La richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, inoltre è necessario informare l'individuo degli obiettivi del trattamento dei dati personali. Infine l'interessato deve aver modo di revocare il proprio consenso in qualunque momento con la stessa facilità con cui l'ha sottoscritto.

6. Diritti degli interessati (di rettifica e di oblio)

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati non corretti o non graditi e la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo
9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento

7. *Comunicazione diretta all'interessato della violazione dei propri dati personali (Data Breach)*

In caso di una violazione dei dati personali l'azienda deve tempestivamente, senza ingiustificato ritardo, comunicare l'accaduto non soltanto alle autorità giudiziarie, ma anche all'interessato.

8. *Piano di implementazione per la protezione dei dati personali*

L'azienda deve impostare un piano di miglioramento basato sui rischi evidenziati nella fase di PIA.

Lo stesso GDPR tuttavia tiene in considerazione la necessità di ponderare e distinguere la portata delle misure a protezione dei trattamenti anche in base alle dimensioni e al fatturato aziendale, prevedendo riferimenti alle esigenze specifiche delle micro, piccole e medie imprese e investendo esplicitamente anche associazioni e organismi rappresentativi delle categorie di titolari del trattamento o responsabili del trattamento del compito di ragionare su, e di contribuire alla corretta applicazione del GDPR stesso.

9. Messa in atto delle misure tecniche ed organizzative di sicurezza

Sulla base del piano di miglioramento, l'Azienda deve passare all'attuazione concreta ed operativa delle :

- misure tecniche e infrastrutturali
- misure organizzative e gestionali
- Info-formazione

10. *Sistema sanzionatorio*

L'articolo 83 del GDPR stabilisce espressamente un sistema sanzionatorio estremamente rigido e pesante che viene definito "dissuasivo"; nei fatti significa che l'entità delle sanzioni può raggiungere i 20 milioni di euro e, nel caso delle violazioni più gravi, arrivare fino al 4% del fatturato totale annuo.

CONCLUSIONI

Le novità apportate dal nuovo Regolamento Europeo sulla Protezione dei Dati Personali 679/2016 sono complesse e richiedono alle aziende uno sforzo per raggiungere un duplice obiettivo: tutelare e garantire la protezione della privacy e ammodernare la propria struttura tecnica organizzativa. In un'azienda ben strutturata i dati sono reperibili più facilmente e questo rende numerosi processi aziendali più snelli nello svolgimento.

Le novità introdotte possono essere vissute come minacce per l'azienda, ma con un giusto approccio si possono trasformare in opportunità, come per esempio:

- la fidelizzazione dei propri clienti, i quali si sentiranno più tutelati;
- una migliore archiviazione e una miglior reperibilità dei dati;
- un rafforzamento dei propri sistemi di sicurezza.

Dimedp Consulting può aiutarti a raggiungere il vostro obiettivo trasformando queste potenziali minacce in reali opportunità con un approccio snello ed efficace attraverso alcuni semplici passaggi:

1. Censimento di tutti i trattamenti effettuati ed individuazione del titolare, dei responsabili e degli incaricati al trattamento dei dati;
2. Mappatura dei rischi che gravano sui trattamenti e valutazione delle misure «adeguate» ai sensi dell'Art. 32 del GDPR (General Data Protection Regulation);
3. Valutazione ed eventuale redazione del registro delle attività di trattamento ai sensi dell'Art. 30 GDPR;
4. Gap Analysis delle attuali informative con adeguamento al GDPR;
5. Definizione delle istruzioni per il titolare, i responsabili e gli incaricati al trattamento dei dati e relativi criteri di controllo e vigilanza;
6. Formazione ai dipendenti in merito alla Privacy e al Nuovo Regolamento 2016/679.
7. Con TEAMSYSTEM AGYO PRIVACY si potrà avere uno strumento software per gestire le azioni e adempimenti necessari in ottemperanza al Regolamento GDPR