NUOVO REGOLAMENTO EUROPEO PRIVACY

Il 24 maggio 2016 **è entrato ufficialmente in vigore il Regolamento dell'Unione Europea n. 2016/679 sulla protezione e libera circolazione dei dati personali** che diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018.

Tale regolamento, le cui disposizioni **sono già obbligatorie**, abroga la Direttiva 95/46/CE (regolamento generale sulla protezione dei dati) e ha lo scopo di rafforzare i livelli di sicurezza, riservatezza e protezione dei dati personali delle persone fisiche e di uniformare la normativa privacy in tutti gli Stati dell'UE.

In Italia, esso coesisterà con il D.Lgs 196/2003 ("Codice Privacy") fino al 25 Maggio 2018 che verrà in tale data abrogato.

Continueranno comunque ad avere efficacia legislativa i provvedimenti del Garante per la Protezione dei Dati Personali

ALCUNE NOVITÀ DEL NUOVO REGOLAMENTO UE 2016/679

Responsabilizzazione ("accountability") del Titolare del Trattamento (Art. 24)
Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative **adeguate ed efficaci** per **garantire**, ed essere in grado di **dimostrare** la conformità del trattamento alle disposizioni normative.

Rispetto al D.Lgs 196/2003, che indicava un livello minimo di sicurezza prescrivendo delle "misure minime", il Regolamento 2016/679 lascia al Titolare del Trattamento l'onere di individuare, implementare e monitorare le misure che ritiene più adeguate. Tale apparente flessibilità comporta quindi un aumento di responsabilità e di impegno organizzativo.

Privacy by design e protezione di default (Art.25)
È obbligatorio gestire gli adempimenti privacy a partire dalla progettazione dei processi aziendali e degli applicativi informatici di supporto mettendo in atto dei meccanismi per garantire che siano trattati - di default - solo i dati personali necessari per ciascuna finalità specifica del trattamento
Ciò comporta l'obbligo per i Titolari del trattamento di prevedere meccanismi di protezione dei dati fin dalla progettazione delle attività e per l'intera gestione del ciclo di vita dei dati.

Data Breach Notification: obbligo di segnalazione in caso di violazione dei dati (artt. 33 e 34)
In caso di violazione dei dati personali (distruzione, perdita, comunicazioni non autorizzate, etc.) il Titolare del Trattamento dovrà provvedere, attraverso i propri Responsabili, alla notificazione della violazione all'Autorità di controllo e alla segnalazione al diretto interessato.

Diritto all'oblio (Art. 17)
L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di provvedere alla loro cancellazione senza ingiustificato ritardo.

Registri delle attività di trattamento (Art. 30)
Introduzione dell'obbligo, per ogni azienda titolare del trattamento dei dati, di tenere un "registro delle attività di trattamento", svolte sotto la propria responsabilità, nonché quello di effettuare una "valutazione di impatto sulla protezione dei dati".
Obbligo di Designazione del Responsabile della protezione dei dati personali (Privacy Officer) (Art. 37)

Il compito del Privacy Officer è quello di consentire al Titolare del Trattamento di assolvere a tutti gli obblighi in materia di protezione dei dati personali (codice privacy, nuovo regolamento UE, provvedimenti del Garante per la Protezione dei Dati Personali).
La sua è obbligatoria ogniqualvolta:

1. il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
2. le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, **richiedono il monitoraggio regolare e sistematico degli interessati su larga scala**;
3. le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel **trattamento, su larga scala, di categorie particolari di dati personal**i (che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) o di dati relativi a condanne penali e a reati.

per stabilire se un trattamento sia effettuato o meno su larga scala occorre tener conto dei seguenti fattori:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento
- la durata, ovvero la persistenza, dell'attività di trattamento
- la portata geografica dell'attività di trattamento.

La nomina del Privacy Officer costituisce una misura adeguata ed efficace per garantire l'accountability (Art. 24) ed è pertanto consigliabile anche nei casi in cui non siano presenti elementi che la rendano obbligatoria.

Infatti, già l'art. 29 del D.lgs 196/2003 dispone che Il Responsabile del trattamento dei dati personali deve essere "*individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza*";
Nominando come Responsabile un professionista esterno, il Titolare del trattamento dei dati personali, ha la possibilità di delegare non soltanto tutti gli obblighi in materia di sicurezza e protezione dei dati personali ma anche le relative responsabilità che attualmente gravano su di Lui. Inoltre tale delega rappresenta la prima e più efficace delle prove a discarico ai sensi dell' art. 2050 del Codice Civile

Il **Responsabile della protezione dei dati personali** deve avere i seguenti requisiti:

- essere "designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e della prassi in materia di protezione dei dati personali e delle capacità di assolvere ai propri compiti" (art. 37, comma 5);
- "non dare adito a conflitti di interessi"; (art. 38, comma 6)
- avere adeguata competenza poiché deve essere in grado soddisfare le richieste degli "Interessati che possono contattarlo per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal regolamento privacy UE". (art. 38, comma 4)

Si evince quindi la necessità di nominare quale responsabile della protezione dei dati personali un professionista che garantisca il soddisfacimento di tali requisiti evitando, tra l'altro, la responsabilità per culpa in eligendo e in vigilando nonché ingenti sanzioni amministrative e penali

ALCUNE SANZIONI

D.Lgs 196/2003

- ✓ Omessa o inidonea informativa (Art. 161) è punita con il pagamento di una somma da seimila euro a trentaseimila euro o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi (…) di maggiore rilevanza per uno o più interessati, da 10.000 € a 60.000 € (Art. 162). La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.
- ✓ L'impropria conservazione del traffico comporta una sanzione da 10.000 € a 50.000 € (Art. 162 bis)
- ✓ L'omessa o incompleta notificazione al Garante comporta una sanzione da 20.000 € a 120.000 € (Art. 164 bis)
- ✓ Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante è punito con la sanzione amministrativa del pagamento di una somma da 20.000 € a 120.000 € (art. 164 D.Lgs 196/2003);
- ✓ Cessione dei dati in violazione dell'art. 16 del D.Lgs 196/2003: Sanzione da 10.000 € a 60.000 €
- ✓ Chiunque, essendovi tenuto, non osserva i **provvedimenti adottati dal Garante** è punito con la reclusione da tre mesi a due anni (art. 170 D.Lgs 196/2003);

Il Regolamento Ue 2016/679 ha stabilito che l'ammontare delle sanzioni amministrative pecuniarie potranno arrivare fino ad un massimo di 20 milioni di Euro o fino al 4% del fatturato

L'Autorità Garante svolge la propria attività ispettiva direttamente o tramite la collaborazione del Nucleo Speciale Privacy della Guardia di Finanza, attivo su tutto il territorio nazionale, e - ove necessario - di altri organi dello Stato.

APTA Servizi Professionali Srl ha esperienza pluriennale nella gestione di tutte le problematiche connesse al Trattamento dei Dati Personali ed è quindi in grado di fornire una consulenza di alto profilo ai Titolari del Trattamento.

I suoi soci si sono abilitati come Privacy Officer Qualificati superando a pieni voti lo specifico master "Privacy Officer & Consulente della privacy" accreditato dal Consiglio Nazionale Forense presso il Ministero della Giustizia e valido ai sensi della Legge 4/2013

Ha inoltre sviluppato un modello gestione per la Protezione dei Dati personali che consenta di implementare correttamente gli adempimenti cogenti in tale ambito attraverso la definizione di opportuni processi, procedure e schemi di auditing.

Garantisce inoltre l'integrazione di tale modello di gestione con quelli eventualmente esistenti in ambito ISO 9001:2015, ISO 14.001:2015 e BS OHSAS 18001:2007.