Circolare informativa
<<Gestione e Organizzazione>>

31 Gennaio 2018

OGGETTO: REGOLAMENTO EUROPEO PRIVACY (ADEGUAMENTO ENTRO IL 25 MAGGIO 2018)

Introduzione

Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla "protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati" stabilisce taluni diritti fondamentali per gli interessati (Informazione, Accesso, Rettifica, Oblio, Limitazione di trattamento, Portabilità, Opposizione) e principi per le aziende, introducendo nuovi obblighi, una nuova figura professionale (Data Protector Officer) e un nuovo e pesantissimo trattamento sanzionatorio.
Il Regolamento abroga la Direttiva 95/46/CEE e si applicherà a partire dal 25 maggio 2018 a tutte le aziende aventi almeno uno stabilimento nell'UE che trattano in modo integrale o parziale, automatizzato o non, i dati personali, indipendentemente dal fatto che il trattamento sia effettuato all'interno dell'Unione.

Tra le numerose attività che le aziende dovranno porre in essere entro la suddetta data, si segnala, in particolare, l'introduzione della figura del Responsabile della Protezione dei Dati (D.P.O.), che dovrà essere obbligatoriamente presente:

- nelle aziende pubbliche quando effettuano il trattamento di dati personali;
- in tutte le aziende dove i trattamenti presentino specifici rischi (aziende nelle quali sia richiesto un monitoraggio regolare e sistematico degli "interessati", su larga scala, o aziende che trattano "dati sensibili, sanitari, genetici e biometrici").

Il D.P.O. potrà essere un dipendente della società Titolare del trattamento o un soggetto esterno avente con la società un contratto di servizi: in ogni caso dovrà essere un professionista competente in tema di protezione dati, in possesso di specifici requisiti quali competenza, esperienza, indipendenza e autonomia di risorse. Ogni azienda dovrà rendere noti i dati del proprio D.P.O. e comunicarli al locale "Garante per la protezione dei dati personali".

Il Responsabile della Protezione Dati dovrà riferire direttamente ai soggetti apicali della società, senza intermediazioni, e con grande autonomia e indipendenza rispetto agli altri dirigenti.

Un altro elemento di novità del nuovo Regolamento europeo è il principio del privacy impact assessment (P.I.A.).
Il P.I.A. è fondamentale nei casi di utilizzo di nuove tecnologie o, comunque, in tutti i casi in cui vi sia un rischio elevato per i diritti e le libertà delle singole persone. In caso di redazione di tale documento, il titolare del trattamento deve, prima di procedere, e confrontandosi qualora vi sia, con il Data Protection Officer, effettuare una valutazione preventiva dell'impatto che può avere il trattamento sulla protezione dei dati personali.
La valutazione avrà ad oggetto:

- la descrizione dei trattamenti che si prevede saranno svolti;
- le finalità del trattamento;
- l'interesse legittimo per il quale il titolare effettua i trattamenti;
- la valutazione della necessità e della proporzionalità del rischio per i diritti e libertà dei soggetti interessati;
- le misure di sicurezza e le garanzie da adottare.

Nel caso in cui dalla valutazione preventiva si evinca un rilevante rischio conseguente al trattamento e si sia in assenza di misure volte a contrastarlo, il titolare interessato è tenuto a chiedere consulto al Garante prima di dare inizio al trattamento stesso.

Inoltre, tutti i soggetti pubblici e privati avranno l'obbligo di provvedere alla:

- definizione organigramma ruoli di responsabilità e redazione dei rispettivi incarichi (interni ed esterni);
- redazione ed aggiornamento del Registro dei Trattamenti;
- redazione di tutta la documentazione necessaria, richiesta da determinate procedure obbligatorie (regolamento interno, informative e consensi, procedura Data Breach, procedura Privacy by Default, procedura risposta richieste degli interessati a esercitare i propri diritti, clausole contrattuali);
- obbligo di formazione annuale ai dipendenti;
- revisione annuale della conformità al GDPR, ossia revisione di tutta la documentazione e del rispetto delle procedure.

Il mancato rispetto dei suddetti adempimenti comporterà l'applicazione di:

- sanzioni amministrative pecuniarie fino a euro 10.000 (o, per le aziende, fino al 2% del fatturato mondiale totale annuo dell'anno antecedente), per la violazione di specifici obblighi imposti dal nuovo Regolamento;
- sanzioni amministrative pecuniarie fino a euro 20.000 (o, per le aziende, fino al 4% del fatturato mondiale totale annuo dell'anno antecedente), per la violazione di più rigidi obblighi imposti dal nuovo Regolamento o per il mancato rispetto degli ordini dettati dal Garante.

In ambito penale vige la competenza del singolo Stato, data l'impossibilità di una previsione del diritto dell'Unione europea. Perciò, entro il 25.5.2018, i singoli Stati membri dovranno stabilire la disciplina da applicare in materia di sanzioni, differenti da quelle amministrative pecuniarie, da irrogare in caso di violazione del nuovo Regolamento, oltre a fornire tutta una serie di chiarimenti in merito alle questioni ancora da dettagliare.

CDA - Studio Legale Tributario vanta un'esperienza ultra ventennale in materia di privacy e si propone di fornire, attraverso consulenti specializzati e formati in tale ambito, una valutazione attenta e puntuale dell'attuale stato di adeguamento privacy della Sua azienda/Ente, pianificando il percorso più idoneo per adempiere nei tempi prefissati agli obblighi previsti dal Regolamento UE Privacy (GDPR).

CDA Studio Legale Tributario