TCL ADVISORS
STUDIO ASSOCIATO

EURODATA 1988 SYSTEMS SRL

Newsletter n. 2/2018

Applicazione della nuova normativa sulla privacy ("Regolamento UE 2016/679" - GDPR - General Data Protection Regulation)

Premessa

A partire dal 25 maggio del 2018 sarà pienamente applicabile il nuovo "Regolamento UE 2016/679" (GDPR - General Data Protection Regulation), entrato in vigore il 25 maggio 2016.

Finalità del provvedimento

Disciplinare la protezione dei dati personali delle persone fisiche e le modalità di circolazione di tali dati da parte dei soggetti che ne effettuano il trattamento con criteri omogenei nei vari paesi membri mediante:

- Il rafforzamento dei diritti dell'interessato ("diritto di accesso, di rettifica, di opposizione e diritto all'oblio")
- un nuovo regime di informativa per l'interessato;
- il divieto al trasferimento di dati personali verso paesi extra UE, salvo che siano rispettati determinati requisiti;
- la comunicazione obbligatoria di eventuali violazioni dei dati personali (data breach);
- l'inasprimento del sistema sanzionatorio con un aumento dell'ammontare delle sanzioni amministrative pecuniarie fino ad un massimo di 10 milioni di Euro o 2% del fatturato mondiale totale annuo, oppure 20 milioni di Euro o 4% del fatturato mondiale totale annuo, a seconda delle violazioni delle disposizioni del Regolamento.

Destinatari

P.A., enti, imprese di qualunque tipo e dimensione, compresi gli studi professionali. Non sono soggetti alla normativa i privati che gestiscono dati per uso strettamente personale.

Vigenza del provvedimento

E' entrato in vigore il 25 maggio 2016 e sarà pienamente applicabile dal 25 maggio 2018. Il Regolamento Europeo è cogente per tutti gli stati membri e si affianca alla normativa nazionale vigente che viene integrata dalla nuova normativa.

Interventi per adempiere al provvedimento

Per raggiungere tali obiettivi la normativa non prevede misure prescrittive predeterminate ma richiede da parte delle aziende attività valutative del rischio informatico e organizzativo nel processo di gestione dei dati.

In particolare, occorre attuare, con modalità correlate alle dimensioni e alla complessità dell'aziende ed alla tipologia di dati trattati, specifiche verifiche e conseguenti interventi riconducibili nei seguenti ambiti:

1) Governance della Privacy (titolare, responsabile, incaricato, procedure, note operative…).
2) Valutazione dei rischi (adeguatezza dei presidi di controllo già in atto per la tutela della Privacy).
3) Diritti dell'interessato (alla cancellazione, alla portabilità, all'accesso, alla rettifica, all'opposizione…).
4) Data retention: definizione del periodo per i quali i dati vanno mantenuti.
5) Segnalazione violazioni (Data Breach) al Garante e all'interessato (sanzioni in caso di inosservanza).
6) Adozione del Registro dei trattamenti e nomina di un Data Protection Officer per attività di vigilanza.
7) Istruzione e formazione del personale adibito al trattamento.
8) Implementazione di nuovi presidi di controllo per corrispondere alle nuove esigenze di compliance, quali:
    - misure legali per la revisione della modulistica, dell'informativa e del consenso;
    - misure organizzative interne;
    - misure di sicurezza tecnologiche e fisiche per la protezione dei dati.

Il processo di adozione del provvedimento: da obbligo a opportunità

La compliance alla normativa se ben realizzata, in ottica non meramente formale e burocratica, può rappresentare l'occasione per le aziende di migliorare la propria

organizzazione interna, di ridurre tempi di registrazione in caso di non infrequente ridondanza di informazioni rivedendo i dati da trattare secondo criteri di pertinenza, e soprattutto incrementare la consapevolezza aziendale sulla cyber security adottando misure per adeguare la sicurezza dei propri sistemi informativi per ridurre il rischio di perdita o di sottrazione di dati.

Le azioni operative

Un team specialistico che integra competenze legali, gestionali e tecniche è in grado di affrontare l'esigenza di compliance, in modo mirato e correlato con riguardo alla complessità delle singole situazioni.

In tale quadro si potranno coniugare gli adempimenti di legge con il miglioramento dei processi relativi ai trattamenti dei dati, svolgendo le attività di:

- analisi documentale dell'informativa e del rilascio del consenso;
- analisi documentale dei contratti con terze parti e delle clausole di miglior tutela per l'azienda;
- risk assesment e stesura di un modello di governance della privacy;
- adozione di un piano di misure per la sicurezza informatica.