SOLUZIONI AMBIENTE SICUREZZA QUALITÀ

OIKOS

UNI EN ISO 9001:2008
CERTIQUALITY
SISTEMA DI GESTIONE QUALITÀ CERTIFICATO

NUOVO REGOLAMENTO EUROPEO 2016/679 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Il nuovo Regolamento Europeo UE/2016/679 relativo alla "**protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati**", abroga la Direttiva 95/46/CE da cui era disceso il vigente Decreto legislativo n.196/2003 italiano (il cosiddetto Codice della Privacy).

La nuova normativa entrerà in vigore in tutti i paesi dell'Unione europea a partire dal 25 maggio 2018. Durante il periodo transitorio le aziende e gli enti pubblici dovranno rivedere i propri processi di trattamento adattandosi alle modifiche introdotte e i legislatori nazionali dovranno adattare i precedenti atti legislativi alle nuove disposizioni europee.

Il Regolamento UE pone obblighi di compliance particolarmente impegnativi nei confronti dei titolari del trattamento di dati personali: i nuovi adempimenti privacy comportano infatti la riorganizzazione del processi aziendali, la riprogettazione del sistema informativo, la revisione di contratti, deleghe e nomine.

In sintesi i principali cambiamenti introdotti dal Regolamento UE 2016/679 riguardano:

- Il concetto di "accountability" ovvero la responsabilizzazione di titolari e responsabili del trattamento e la necessità di un atteggiamento proattivo nel dimostrare la concreta adozione di misure che assicurino il rispetto del Regolamento

- L'approccio basato sull' analisi preventiva e la valutazione del rischio che un trattamento di dati personali può comportare per i diritti e le libertà degli interessati e la conseguente attuazione di misure di protezione idonee alla limitazione di tale rischio

- La tenuta da parte dei Titolari e dei Responsabili del trattamento del Registro delle attività di trattamento, strumento indispensabile per ogni valutazione e analisi del rischio

- La nuova figura del «Responsabile della protezione dei dati» (*Data Protection Officer* o DPO), obbligatoria per talune categorie di titolari ma prevista anche su base volontaria, incaricato di assicurare una corretta gestione dei dati personali; è il referente, una sorta di presidio per la privacy, dotato di requisiti e competenze elevate, con compiti quali:
    - informare e fornire consulenza al Titolare del trattamento o al responsabile del trattamento e agli addetti al trattamento in merito agli obblighi del Regolamento e di altre disposizioni dell'Unione o nazionali relative alla protezione dei dati
    - sorvegliare il rispetto del Regolamento e di altre disposizioni normative relative alla protezione dei dati personali e delle politiche del titolare del trattamento o del responsabile del trattamento
    - sorvegliare l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale addetto ai trattamenti e alle connesse attività di controllo
    - fornire se richiesto un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento
    - cooperare e fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

- Il concetto di *privacy by default* e *by design*, cioè la configurazione di un trattamento prevedendo fin dalla sua progettazione (a livello tecnico e organizzativo) e per impostazione predefinita le garanzie indispensabili per la sicurezza dei dati previste dai requisiti di legge

- La registrazione e la comunicazione all'Autorità di controllo competente dei casi di avvenuta violazione dei dati personali (data breach) in caso di rischi per i diritti e la libertà degli interessati

- La preventiva valutazione di impatto sulla protezione dei dati ("*data protection impact assessment*") relativa ad un trattamento, in particolare se avviene su larga scala, riguarda un numero elevato di interessati e prevede l'utilizzo di nuove tecnologie

- L' adozione di codici di condotta, marchi e schemi di certificazione del trattamento, accreditati dal legislatore nazionale, quale elemento per dimostrare la conformità dei trattamenti ai requisiti di sicurezza.

Sanzioni

Le sanzioni amministrative previste dal Regolamento danno spazio d'azione ai Garanti nazionali: nelle ipotesi di minor gravità possono limitarsi a un ammonimento, senza strascichi pecuniari.

Il Regolamento prevede però che circa la metà delle prescrizioni sia assistita da sanzioni amministrative, tra l'altro molto elevate. Sono applicabili due fasce sanzionatorie in relazione al tipo di violazione: la prima ha come massimo imputabile l'importo di 10 milioni di euro e la seconda di 20 milioni di euro. Senza contare che tali cifre possono ulteriormente incrementarsi per le imprese, se si applica la sanzione in misura percentuale, pari rispettivamente al 2% o al 4% del fatturato mondiale globale annuo. La misura percentuale si applica nel caso in cui sia superiore alla misura fissa.

☎ Per ulteriori informazioni ed approfondimenti:
Oikos s.c.r.l., Strada Cavagnari 12/A – 43126 PARMA
Tel/fax: 0521 291590
www.oikos-scrl.it
Rif: dott.ssa Roberta Zampiccinini, zampiccinini@oikos-scrl.it
dott.ssa Monica Galliani: galliani@oikos-scrl.it
Scheda n. 27 - Aggiornata a ottobre 2017