PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3871 di martedì 11 ottobre 2016

Il sistema di gestione della protezione dei dati personali

Il Regolamento Europeo 679/2016 richiede analisi di rischio e procedure specifiche: quali sono le peculiarità e le opportunità che offre un Sistema di Gestione per la Protezione dati Personali? Di Paola Limatola e Sebastiano Plutino.

Il Regolamento EU 679/2016, in vigore dal 24 maggio 2016, in materia di trattamento dei dati personali stabilisce che il Titolare del Trattamento di Dati Personali debba predisporre misure adeguate per proteggere le informazioni personali fin dalla fase di progettazione di un servizio o di un processo, anche attraverso l'utilizzo di impostazioni predefinite, quali ad esempio la minimizzazione dei dati già in fase di raccolta o la cancellazione automatica delle informazioni in coincidenza con la scadenza dei termini di conservazione dichiarati nell'informativa.

Le organizzazioni sono quindi chiamate a dedicare al tema della protezione dei dati personali un'attenzione più ampia, conducendo, ove necessario, analisi di rischio o, in casi specifici, dotandosi di un registro dei trattamenti.

Più in generale, ogni organizzazione deve:

- valutare attentamente la propria situazione specifica e il contesto in cui opera;

- identificare le caratteristiche del trattamento effettuate;

- adottare misure tecnico-organizzative che garantiscano un livello di protezione adeguato tutelando fin dall'inizio i diritti dell'interessato.

Ciascuna organizzazione dovrà inoltre:

- verificare le clausole dei contratti stipulati con i propri fornitori di servizi per assicurarsi che le operazioni di trattamento avvengano secondo la corretta attribuzione di ruoli e responsabilità, come richiesto dal Regolamento

- istruire il personale interno,

- predisporre procedure per rispondere alle richieste dei clienti in merito ai propri dati e conservare tutta la documentazione relativa, così da poterla esibire in caso di richiesta dell'Autorità preposta;

- conservare la documentazione attestante la liceità del trattamento effettuato;

- organizzarsi per rispondere alle eventuali richieste dell'Autorità;

- definire metodi documentati per gestire eventuali violazioni dei dati;

- monitorare costantemente lo "stato di salute" dei propri processi e dei trattamenti su dati personali, anche per identificare possibili manomissioni o intrusioni;

- recepire prontamente gli aggiornamenti normativi che dovessero man mano intervenire.

Tutti questi elementi configurano, per l'organizzazione, l'opportunità di dotarsi di un **sistema di gestione della protezione dei dati personali**.

La protezione dei dati personali, considerati non solo i recenti e spiacevoli fatti di cronaca che hanno richiamato l'attenzione pubblica ma anche la crescente complessità dei sistemi IT, la diffusione della tecnologia mobile, il frequente ricorso a servizi di outsourcing e l'utilizzo diffuso di sistemi *cloud* (che possono rendere più difficoltoso identificare con sicurezza il luogo fisico di conservazione del dato), non può essere considerata un fattore marginale ma sta diventando sempre più una priorità.

Un sistema di gestione della protezione dei dati personali, strutturato ad esempio sulla base dei requisiti generali indicati nel DPMS (Data Protection Management System) 44001©:2016, deve essere allineato agli obiettivi dell'impresa, adeguato al contesto specifico e dovrebbe rispondere alle esigenze di tutte le realtà organizzative, coinvolgendole e fornendo indicazioni chiare a tutti gli attori del trattamento. Inoltre, all'interno dell'organizzazione, deve favorire lo sviluppo di una cultura d'impresa diffusa, a cui tutte le funzioni aziendali si sentono chiamate a partecipare.

L'applicazione di un sistema di gestione della protezione dei dati personali terrà conto delle dimensioni dell'organizzazione, del settore di mercato in cui opera e della quantità di dati personali trattati; permetterà di governare ogni aspetto dei processi legati al trattamento di dati personali; introdurrà un processo di miglioramento continuo che porterà benefici in termini di ritorno economico dell'investimento.

L'adozione di un sistema di gestione della protezione dei dati personali aiuta le imprese ad applicare correttamente le norme e ad agire virtuosamente. La conformità al Regolamento deve essere percepita dalle organizzazioni come un vantaggio competitivo e non un mero costo.

Consumatori, clienti e associati (gli interessati), ovunque residenti in Europa, premieranno le organizzazioni che, in modo trasparente, saranno in grado di garantire un elevato livello di tutela delle informazioni personali, anche mediante attestazioni di entità indipendenti a seguito di monitoraggi mirati (limitati cioè a pochi documenti obbligatori) o globali del sistema di gestione adottato.

L'impegno al raggiungimento della conformità ? dimostrabile attraverso l'adozione di un apposito sistema di gestione e controllo e/o attraverso l'ottenimento di certificazioni terze - rafforza la reputazione dell'organizzazione sul mercato e le permette di proporsi ai potenziali clienti quale interlocutore affidabile.

In un'Europa sempre più attenta alla protezione ed alla difesa dei suoi principi fondanti, questo rappresenterà un valore ancor più

rilevante con l'entrata in vigore del Regolamento Europeo sulla protezione dati.

Paola Limatola

Sebastiano Plutino

Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
