Adeguarsi al GDPR: tra obblighi e opportunità

Author : Andrea Battistella

Date : 16 maggio 2018

Il regolamento Europeo sul trattamento dei dati personali, segnerà un grande cambiamento nella gestione dei dati personali e nell'approccio al diritto alla privacy.

L'adeguamento alla nuova normativa Europea, comporterà inevitabilmente un'operazione di riprogettazione di quei processi aziendali che hanno ad oggetto il trattamento dei dati personali.

Analizzare, valutare, documentare e aggiornare saranno le azioni che caratterizzeranno ogni attività di adeguamento; infatti, il GDPR richiede, ad ogni titolare del trattamento, di implementare all'interno della propria organizzazione le misure organizzative e tecniche adeguate per garantire che il trattamento dei dati personali avvenga in conformità con quanto disposto dalla normativa stessa.

Rispetto al passato, la scelta delle misure organizzative e tecniche da attuare potrà essere effettuata in modo libero e senza i limiti imposti dalla normativa. Nel GDPR, infatti, non vengono elencate le misure minime di sicurezza da attuare, così come veniva specificato nel Codice della privacy e nell'allegato B.

Il prossimo 25 maggio, quindi, ogni Titolare del trattamento avrà sul suo tavolo un foglio bianco che, tenuto conto della natura, dell'ambito del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, dovrà compilare con tutte quelle informazioni necessarie per delineare e descrivere il proprio modello organizzativo privacy.

La libertà che il GDPR riconosce ad ogni titolare del trattamento è però bilanciata dall'obbligo di documentare e provare le analisi, le valutazioni fatte e le scelte che sono state prese per organizzare e proteggere i dati personali.

Il Titolare del trattamento, quindi, dovrà assumere un atteggiamento attivo e responsabile ed ogni decisione relativa al trattamento dei dati dovrà essere ponderata e documentata.

A supporto dell'accountability, il GDPR, all'articolo 30, prevede il documento denominato

Registro dei Trattamenti, che, di fatto, è l'unico documento che il titolare del trattamento è obbligato, solo in alcuni casi, a predisporre e tenere, ma che è anche l'unico documento, che, a prescindere da detto obbligo, permette di documentare il modello organizzativo privacy adottato. Quindi il registro dei trattamenti è uno strumento necessario per mantenere il controllo della propria organizzazione e per poter dimostrare che il trattamento dei dati è realmente effettuato.

Dal punto di vista pratico, la domanda che ogni titolare si deve porre è: "come attuare quanto richiesto dalla nuova norma europea?"

I principali adempimenti, come informativa, consenso e misure di sicurezza, non subiscono grandi cambiamenti rispetto a quanto previsto dal Codice della privacy. L'elemento di discontinuità è rappresentato dalla modalità di attuazione; gli adempimenti privacy dovranno essere visti non più come adempimenti formali, bensì dovranno essere attuati in modo concreto. Il punto di partenza di ogni processo di adeguamento dovrà essere il principio privacy by design, cioè il Titolare del trattamento, prima ancora di pensare a come adeguarsi, dovrà programmare il trattamento che dovrà essere avviato. La tutela della privacy dovrà essere attuata preventivamente e dovrà essere il risultato di un approccio proattivo del Titolare del trattamento.

Gli articoli 24 e 32 del GDPR, individuano la metodologia da seguire per disegnare ed organizzare un modello organizzativo privacy conforme alla normativa; infatti, dagli adempimenti prescritti dall'art. 24 si possono ipotizzare le seguenti fasi del processo di adeguamento:

1 - Valutazione: il Titolare del trattamento, mappando la propria organizzazione, dovrà, come prima cosa, censire e analizzare quello che accade all'interno della propria azienda. Quindi, dovranno essere individuati:

- il contesto in cui è effettuato il trattamento dei dati;
- la natura dei dati trattati;
- le finalità perseguite con il trattamento dei dati (la finalità del trattamento rappresenta l'obiettivo che ogni titolare vuole raggiungere tramite l'utilizzo dei dati personali. Definire la finalità è fondamentale per capire quali dati si devono realmente raccogliere per effettuate il trattamento, quali informazioni fornire all'interessato e quale dovrà essere il contenuto del consenso che nel caso si dovrà richiedere);
- l'organigramma privacy, definendo ruoli e responsabilità.

2 - Attuazione: Dall'analisi della propria organizzazione, il titolare dovrà predisporre un piano di adeguamento al fine di colmare il gap normativo. Nel piano di adeguamento dovranno essere individuate le misure organizzative e tecniche da attuare. La scelta delle misure adeguate dovrà essere effettuata tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche.

3 - Verifica: Il titolare, dopo l'attuazione delle misure di sicurezza, dovrà verificare e

documentare le scelte, le analisi e le valutazioni fatte; in questo modo il titolare creerà un proprio sistema documentale privacy necessario per provare quanto attuato e per gestire la successiva fase dell'aggiornamento.

4 - Aggiornamento: Al fine di rendere il modello organizzativo privacy sempre adeguato alla normativa, il titolare dovrà verificare periodicamente eventuali cambiamenti nelle modalità di trattamento e, nel caso, aggiornare il modello e la documentazione descrittiva.

Il titolare del trattamento, quindi, dovrà, con la massima libertà, individuare quelle procedure atte ad analizzare e valutare la propria organizzazione, al fine di definire poi un modello organizzativo e di gestione della privacy finalizzato a proteggere i dati personali ed i diritti degli interessati dalle minacce e dai rischi individuati.

Alla fine di questo processo di adeguamento, il titolare dovrà essere in grado di dimostrare e descrivere, tramite specifica documentazione: il proprio modello aziendale, le misure organizzative e tecniche attuate, le istruzioni per trattare i dati personali alle persone autorizzate. Nel caso di trattamento basato sul consenso dell'interessato, il titolare dovrà organizzare e conservare le dichiarazioni di consenso, in modo da garantire, in caso di accertamenti e/o di richieste da parte degli interessati, la ricercabilità e l'esibizione di dette dichiarazioni di consenso.

Il ciclo di attività finalizzate all'adeguamento normativo è sicuramente molto vicino ai modelli di gestione a cui le aziende aderiscono in modo volontario, come ad esempio quelli sulla qualità (ISO 9001) e rappresenta anche l'opportunità, per ogni titolare del trattamento, di riorganizzare i propri processi aziendali anche in ottica di miglioramento dell'efficacia ed efficienza dei rispettivi processi.

Inoltre, altro aspetto da considerare in ottica di adeguamento GDPR, è quello di considerare che trattare i dati personali in modo illegittimo può rappresentare un danno di immagine e reputazionale importante.

In questo momento storico l'opinione pubblica ha alzato l'attenzione sull'utilizzo illegittimo dei dati personali per finalità di business, ne è un esempio la vicenda di Facebook e Cambridge Analytica.

Diventa, quindi, essenziale raccogliere i dati personali in modo trasparente e chiaro, fornendo all'interessato tutte le informazioni previste dalle normative e necessarie per far conoscere le finalità e le modalità del trattamento.

Infatti, gestire i dati rispettando i principi richiamati dalla normativa, vuol dire anche migliorare la propria reputazione e instaurare con gli interessati rapporti commerciali chiari, trasparenti e rassicuranti.

In conclusione, possiamo dire che se il lavoro di adeguamento al GDPR passerà per l'applicazione dei principi di Privacy by design, Privacy by default e accountability, inevitabilmente il Titolare del trattamento, oltre ad aver attuato quanto disposto della normativa,

avrà l’occasione di ottenere effetti positivi in termini di efficienza organizzativa e di accrescere o migliorare il rapporto di fiducia instaurato con gli interessati quali clienti, prospect, fornitori e dipendenti.

A cura di: **Andrea Battistella**