Gestione. L'applicazione del regolamento europeo 2016/679 a partire dal 25 maggio 2018 costringe le imprese ad attivarsi

Privacy, al lavoro per il budget

Primi passi: la mappatura dei dati, degli adempimenti e dell'assetto tecnico-organizzativo

Riccardo Imperiali
Rosario Imperiali

L'ultima notizia è di qualche giorno fa e riguarda Uber, la società statunitense che gestisce l'applicazione per prenotare automobili con autista: circa un anno fa avrebbe subito l'hacker-aggio dei dati di 57 milioni di utenti nel mondo, di cui 600mila conducenti. Ma ormai quasi quotidianamente arriva l'eco di accessi a siti e applicazioni di aziende e, cosa più preoccupante, istituzioni pubbliche con conseguente "furto" dei dati personali degli utenti, che stanno diventando sempre più la vera ricchezza di questa era digitale. Questo è sufficiente per far comprendere come il tema del trattamento dei dati personali sia pressante e come l'applicazione del regolamento europeo 2016/679 a partire dal 25 maggio 2018 (noto anche come Gdpr, acronimo di General data protection regulation) diventi centrale per le imprese.

IL PUNTO DI PARTENZA
Con il supporto di un esperto si valuterà la conformità attuale con l'accertamento del delta differenziale rispetto a quanto prescritto dal Gdpr

Nonostante il termine per mettersi al pari sembri lontano, la materia è complessa e i cambiamenti che apporta il regolamento consistenti, per cui è buona cosa cominciare prima possibile.

Il censimento dei trattamenti e delle rispettive componenti essenziali (mappatura), insieme alla ricognizione degli adempimenti e delle misure tecnico-organizzative adottate rappresentano i primi passi che consentono all'azienda, con il supporto di un esperto della materia, di valutare lo stato di conformità attuale (stato dell'arte) insieme all'accertamento del delta differenziale rispetto a quanto prescritto dal Gdpr (valutazione delle carenze). La lista delle carenze, con l'attribuzione a ciascuna di un indice di rilevanza, permette di individuare le azioni di rimedio e di pianificarne l'implementazione, secondo un ordine di priorità ed una tempistica predefinita.

Questa modalità rende possibile determinare con sufficiente accuratezza alcuni elementi fondamentali per la gestione del relativo progetto aziendale: cioè, quali e quante risorse interne occorrono, qual è il budget stimato, quali sono le interdipendenze tra un'attività e l'altra, quali gli artefatti o i risultati attesi nei diversi stati di avanzamento lavori, come facilitare l'assimilazione dei risultati da parte del tessuto aziendale interno, evitando contraccolpi o negligenze.

La rilevazione delle carenze inevitabilmente rivelerà qualche mancanza rispetto alla normativa vigente ed altre riguardo alle future prescrizioni del Gdpr, ponendosi l'interrogativo di come comportarsi nei riguardi di quelle mancanze che cesseranno di essere tali con il Gdpr (ad esempio, l'obbligo di notificazione preventiva al Garante); al riguardo occorrerà tener presente che in proposito vige il principio per cui l'atto è soggetto alla norma vigente al momento in cui è stato compiuto: cioè, se la notificazione è dovuta ora ma non lo sarà più dopo maggio 2018, la mancanza non sarà sanata per il periodo in cui la stessa notificazione era obbligatoria. Completeranno i rimedi quelli dipendenti da nuove prescrizioni del Gdpr, distinguendo le misure tecniche (come la maggior parte delle misure di sicurezza) dalle organizzative (ad esempio, il modello organizzativo dei ruoli data protection) e tra quelle di natura documentale (come informative, modelli contrattuali, registro dei trattamenti e dei data breach) o di processo (approccio basato sul rischio, impostazione in fase di progettazione, gestione delle violazioni, valutazioni e Dpia).

© RIPRODUZIONE RISERVATA

L'EBOOK

LE NUOVE REGOLE DELLA PRIVACY

Online sul sito del Sole
Dal 28 maggio 2018 entra in vigore il nuovo regolamento europeo sul trattamento dei dati personali, che impatterà in modo considerevole sulla vita delle imprese. Dovranno essere previste nuove figure in organigramma, nuovi adempimenti e nuove modalità per quelli esistenti. Per capire come muoversi Il Sole 24 Ore mette online a disposizione dei lettori un ebook dedicato al tema.

www.ilsole24ore.com/ebook

Il General data protection regulation in dieci passaggi

1	COSA FINISCE SOTTO IL GDPR E QUALE È L'AUTORITÀ GUIDA	Stabilire l'ambito applicativo del Gdpr è di interesse per gruppi multinazionali ma anche per società stabilite nell'Unione europea con fornitori e appaltatori in paesi non-Ue o, viceversa, per società extra Ue che fanno affari	con l'Europa. Analogamente, se l'azienda opera nell'Unione europea o svolge attività con impatti su soggetti Ue, occorre determinare quale sia l'Autorità competente (cosiddetta Autorità guida)
2	IL SISTEMA DOCUMENTALE UTILIZZATO	Il Gdpr si avvale di un articolato sistema documentale con funzione descrittiva e probatoria di quanto realizzato riguardo alle prescrizioni di legge. Vi fanno parte i registri di trattamento e di data breach, la	contrattualistica tra co-titolari, con responsabili e sub-responsabili o per trasferimenti esteri di dati, le Dpia realizzate, le valutazioni del Dpo, informative e modelli di consenso
3	IL MODELLO ORGANIZZATIVO DATA PROTECTION	Il sistema richiede il presidio di ruoli, di legge e volontari, finalizzati ad assicurare l'effettivo funzionamento in contrapposizione a modalità essenzialmente di facciata. Chi opera sui dati personali dovrà	ricevere istruzioni sulle modalità da seguire, ma tra il titolare e gli incaricati – entrambi obbligatori – vi è un vuoto organizzativo da colmare secondo la diligenza imprenditoriale
4	MISURE TECNICHE E ORGANIZZATIVE DA ADOTTARE	La sicurezza, non solo tecnica, assurge a principio: se essa è carente, il trattamento è illegittimo. Le misure vanno scelte ed adottate secondo la responsabilizzazione dell'impresa, comparando rischi individuati	e misure di contrasto per minimizzarli. Servono per prevenire e rimediare i data breach, per ponderare e ridurre il rischio, per facilitare l'esercizio dei diritti e verificare la conformità
5	PROCESSO DI VALUTAZIONE E DPIA	È nota la Dpia, madre delle valutazioni, meno il processo valutativo che permea il sistema; è difficile immaginare un profilo del Gdpr il quale non presupponga una valutazione di adeguatezza:	l'obbligatorietà del Dpo, la necessità di comunicare casi di data breach, la stessa necessità di effettuare una Dpia. La maggiore sfida per l'azienda è mettere in piedi questo processo by design
6	GESTIONE DELL'ESERCIZIO DEI DIRITTI	Il Gdpr chiede all'azienda di facilitare l'esercizio dei diritti da parte degli interessati: tramite la divulgazione informativa, creando canali di accesso noti ed agevoli, garantendo una risposta	esaustiva e tempestiva. Il risultato è frutto di un mix di formazione interna, ingegnerizzazione di processi dedicati e tool informatici di supporto, specie per la ricerca dei dati e la gestione delle richieste
7	PROCESSO DI DATA BREACH	Il data breach "privacy" nasconde numerose insidie: partendo dal concetto di "violazione", che non corrisponde a quello tradizionale del "breach management", sino alla gestione delle comunicazioni a	Garante e interessati, non tassative, ma frutto di una valutazione degli impatti causati. Tra questi estremi si collocano i momenti della rilevazione tempestiva dell'incidente e delle azioni di rimedio
8	GESTIONE DEI TRASFERIMENTI ESTERI	La prassi odierna ha sottovalutato la portata della disciplina dei trasferimenti esteri di dati, limitandosi a delle dichiarazioni generiche nelle informative e all'uso di modelli contrattuali di salvaguardia. Il Gdpr introduce	la necessità di censire, gestire e informare adeguatamente gli interessati con una granularità che arriva sino all'indicazione del Paese destinatario e delle misure di salvaguardia adottate
9	ATTIVITÀ DI FORMAZIONE E SENSIBILIZZAZIONE	Un sistema gestionale è innanzitutto fatto di persone e queste vanno formate e sensibilizzate per evitare il rischio che anche il migliore dei modelli possa rimanere sulla carta e non tradursi in azioni	concrete e prassi comportamentali. Ancorché esistono poche tracce esplicite di tale obbligo nel Gdpr, esso è espressione diretta del principio di responsabilizzazione
10	GESTIONE DELLE TERZE PARTI	L'impresa è "aperta" alla filiera di fornitori, intermediari, appaltatori. Gli affari richiedono flussi continuativi di dati e canali affidabili. Le terze parti utilizzano la materia prima informativa con il rischio di	alterare il bilanciamento di conformità che l'azienda ha ottenuto tramite investimenti; il Gdpr vuole una selezione accorta delle terze parti e il loro assoggettamento a clausole di responsabilità