Il Giornale dell'Ingegnere
Mensile
Data 06-2018
Pagina 20
Foglio 1 / 2

PRIVACY **UNO SGUARDO D'INSIEME**

Il GDPR in 5 mosse

Una normativa di armonizzazione che spinge a ragionare, non tanto e solo sul mero rispetto delle prescrizioni formali e obbligatorie, quanto su scelte e strategie sostanziali con un nuovo approccio proattivo

ING. ROBERTO ORVIETO
AVV. ALBERTO MASCIA

Il Regolamento (UE) n. 679/2016 (General Data Protection Regulation) è dal 25 maggio scorso la normativa direttamente applicabile a livello europeo in tema di trattamento dei dati personali e libera circolazione degli stessi. Ecco una sintesi in 5 punti.

1. FLUSSI DI DATI: ALCUNE CATEGORIE DI DATI

Studi, società, enti, associazioni, effettuano giornalmente uno o più trattamenti di dati personali (es. nome e cognome, codice fiscale, immagini, ecc.). In relazione a tali trattamenti vanno di norma individuate le figure di riferimento (vedi n. 2), predisposte informative ad hoc, sottoscritte eventuali formule di consenso, ove richiesto (vedi n. 4). Vengono, altresì, di norma predisposti processi interni (vedi nn. 3 e 5) che mirano a proteggere tali dati, sin dalla fase di progettazione (Privacy by Design) per un trattamento consapevole e responsabile, e, per impostazione predefinita (Privacy by Default), per un trattamento che non vada oltre i dati necessari per le finalità previste. Per i dati sensibili (il GDPR parla di particolari categorie di dati, tra cui, ad es., l'origine razziale/etnica, le opinioni politiche, i dati genetici e biometrici, la salute, etc.) sono previste maggiori e specifiche cautele (art. 9 GDPR).

2. INDIVIDUAZIONE RUOLI E RESPONSABILITÀ

Il **titolare** (es. la società X, lo studio Y, l'ente Z) è il protagonista delle scelte principali e rilevanti in tema di protezione dei dati, finalità, modalità, mezzi, oltre a essere il destinatario dei principali oneri e responsabilità derivanti dal GDPR.

Il **responsabile del trattamento** (in molti paesi viene imposto che debba essere un soggetto terzo esterno) è designato tra coloro che possano fornire le garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate al fine di assicurare il pieno rispetto delle disposizioni, nonché garantire la tutela dei diritti dell'interessato (affidabilità, conoscenza specialistica, risorse) e, nei casi in cui i dati vengano trattati per conto del titolare, designato con apposito contratto o altro atto giuridico.

L'incaricato al trattamento (es. il dipendente che tratta dati), presente nel Codice Privacy, ma non citato nel GDPR, è inquadrabile nell'organigramma privacy come persona autorizzata al trattamento da parte del titolare e del responsabile, sulla base di specifiche istruzioni a esso fornite.

Il **DPO** (Data Protection Officer) è designato nell'ottica di seguire un percorso di conformità al GDPR e alle altre norme vigenti sulla protezione dei dati. Viene nominato per ragioni di necessità (art. 37 GDPR), ma anche di opportunità, come risorsa preziosa per supportare la funzione di compliance in tema di protezione dei dati.

3. ORGANIZZAZIONE, PROGETTAZIONE E VALUTAZIONE DEI RISCHI

L'organizzazione in tale ambito richiama innanzitutto i concetti di consapevolezza e responsabilizzazione **(Accountability)**. L'Accountability è una componente centrale da valutare con riferimento all'approccio proattivo tenuto dal titolare, e caratterizzato da azioni e misure scelte e applicate per proteggere i dati. Organizzazione significa, anche, pianificazione e strutturazione dei processi che rendono una struttura virtuosa in tema di protezione dei dati personali. Si pensi al processo da attivare in caso di Data breach (violazione dei dati), per rendere effettivo l'esercizio dei diritti dell'interessato (tra cui il diritto alla cancellazione dei dati, oppure, ove previsto, quello alla portabilità degli stessi), ovvero per l'adozione di misure tecnologiche di protezione e sicurezza dei dati. In senso ampio, l'interdipendenza tra protezione e sicurezza dei dati si propone come costante in sede di valutazione dei rischi legata al trattamento degli stessi, con attenzione per i diritti e le libertà delle persone fisiche. La procedura di DPIA (Data Protection Impact Assessment) determina l'origine, la natura, la particolarità e la gravità di tali rischi, al fine di individuare e adottare specifiche misure di sicurezza. Si tratta di una procedura obbligatoria nei casi previsti dal GDPR (v. art. 35), ma che può essere consigliata, al di là dell'obbligatorietà, per il potenziamento e l'ottimizzazione del sistema di protezione dei dati di una struttura.

4. INFORMATIVE, CONSENSI E REGISTRI

Le **informative** vanno redatte ex novo, per nuove tipologie di trattamento di dati, e rinnovate, per trattamenti già posti in essere sulla base di precedenti informative, ove sia necessario adeguarle a quanto prescritto dagli artt. 13 e 14 GDPR. È importante l'efficacia: informative concise, trasparenti, comprensibili, redatte con un linguaggio chiaro e semplice. A tale adempimento sono tenuti tutti coloro che trattano dati, a meno che le informative emesse precedentemente al 25 maggio non abbiano già un contenuto in linea con il GDPR.

Il **Consenso** dell'interessato è tuttora una base giuridica centrale per la liceità del trattamento, sebbene non sia l'unica, ed è ad esempio richiesto come esplicito per il trattamento di categorie particolari di dati (**i dati sensibili**) e per decisioni basate su **trattamenti automatizzati** (compresa la profilazione). Il consenso deve, in linea generale, avere sempre specifici requisiti (inequivocabile, libero, specifico, informato,

granulare, dimostrabile, revocabile). In caso di consenso raccolto prima del 25 maggio – e in linea con tutti i suddetti requisiti –, non è necessario chiederlo nuovamente.
andrebbe creato ed emesso, al di là di ogni ipotesi di obbligatorietà ex GDPR, in quanto è uno strumento prezioso per dimostrare in ottica di adeguamento preventivo, insieme a tutti gli altri profili in esso indicati, la rispondenza di una struttura alle prescrizioni del GDPR e alla corretta gestione dei dati personali.

5. ADEGUATEZZA MISURE TECNICHE-ORGANIZZATIVE E SANZIONI

Le **misure** indicate all'art. 32 GDPR sono, a titolo esemplificativo, la pseudonimizzazione e la cifratura dei dati, la resilienza dei sistemi e dei servizi, il disaster recovery e altro ancora, e vanno adottate in considerazione di specifici fattori (es. la tecnologia disponibile, la natura dei dati, le finalità del trattamento, il rischio per i diritti e le libertà delle persone fisiche, etc.). Un ausilio, nell'individuazione di tali misure adeguate può essere fornito dal Disciplinare tecnico (All. B al Codice Privacy), che per anni è stato preso in esame come il nucleo centrale minimo per garantire la sicurezza dei dati. Un punto di partenza da tenere in considerazione.

In tema di **sanzioni**, il GDPR fa riferimento espressamente a sanzioni amministrative pecuniarie, in relazione alle quali dovranno applicarsi i principi di effettività, proporzionalità e dissuasività. Dovranno altresì trovare applicazione il principio della gradualità (le sanzioni saranno applicate con un approccio graduale) e dell'equivalenza (il livello di protezione dovrà essere equivalente in tutti gli Stati membri). No a facili allarmismi, dunque, no a facilonerie, no ad atteggiamenti orientati alla superficialità e al mero formalismo. Sì a un approccio orientato all'impegno inteso come applicazione concreta, miglioramento, e adeguamento di ogni misura e processo che miri alla valorizzazione dei dati come strategia di migliore organizzazione e competitività commerciale.

Il recente incontro tenutosi lo scorso 17 maggio, presso il Consiglio Nazionale degli ingegneri, ha trattato i temi nello specifico e avviato le basi per la costituzione di un gruppo di lavoro per la delicata materia.