TeLex Anie
NOVITÀ LEGISLATIVE E GIURISPRUDENZIALI
Estratto
N. 5 Anno XXII
Maggio 2017

PRIVACY

LE PRINCIPALI NOVITÀ INTRODOTTE DAL NUOVO REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI PERSONALI

Il 04 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione europea il regolamento (UE) 2016/679, datato 27 aprile 2016, del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali. E' giunto, così, al termine il pacchetto di riforma sulla tutela dei dati personali, presentato dalla Commissione Europea nel 2012, che abroga la direttiva 95/46/CE. Al termine di una vacatio di venti giorni, il regolamento entrerà in vigore, ma sarà applicabile solo a decorrere dal 25 maggio 2018 (articolo 99 Regolamento).

La riforma europea sulla privacy

La **riforma europea** sulla privacy si compone dei seguenti strumenti:

– Il **regolamento** UE 2016/679 sulla protezione dei dati, che abrogherà (vedi articolo 94) l'attuale direttiva 95/46/CE (c.d. direttiva madre). Resta, invece, vigente la Direttiva 2002/58/CE (art.95);

– La **direttiva** UE 2016/680 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché sulla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;

– La **direttiva** UE 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

Le principali novità del nuovo regolamento europeo privacy:

Il quadro normativo delineato dal nuovo regolamento europeo richiede la definizione di *governance* aziendali nel settore della Privacy Security. Sotto questo profilo, è destinata ad assumere sempre più importanza l'implementazione delle misure c.d di *Cyber Security*. Come noto, la *Cyber Security* è una disciplina che si occupa di data security sotto un profilo tecnico-giuridico, con metodologie e soluzioni tipiche dell'informatica giuridica.

Sebbene ad oggi la presa di coscienza dell'importanza della cyber security sia quasi inesistente nel mondo imprenditoriale e non solo, si tratta di un tema che aziende e pubbliche amministrazioni dovranno perseguire in questi due anni di tempo prima dell'applicazione del nuovo regolamento, individuando *roadmap* di implementazione di misure idonee a garantire la sicurezza di sistemi e dati.

Garantire luoghi sicuri, dove custodire e trasmettere informazioni (dati personali), è sicuramente *conditio* sine qua non per fronteggiare i nuovi istituti introdotti dal nuovo regolamento, quali, ad esempio, la data *breach notification*.

Tra le novità principali, introdotte dal nuovo regolamento privacy UE e destinate a giocare un ruolo dominante nelle politiche di *governance*, è doveroso menzionare il principio dell'***accountability***, per effetto del quale, i titolari del trattamento, sia pubblici che privati, dovranno dimostrare, attraverso valutazioni di impatto privacy, di aver effettuato documentati *risk assessment* a tutela dei dati personali.

La valutazione d'impatto sulla protezione dei dati personali (***data protection impact assessment*** – Art. 35 -) è una norma cardine nel sistema privacy del nuovo regolamento UE. Ogni trattamento di dati personali, che presenta rischi per i diritti e le libertà degli individui, deve essere esaminato attentamente. La natura dei dati, la tipologia e la finalità del trattamento e l'applicazione di nuove tecnologie sono alcuni dei fondamentali parametri da valutare. La valutazione di impatto sulla protezione dei dati personali, oltre ad essere obbligatoria quando sono trattati dati sensibili o giudiziari, è dovuta anche nei casi di trattamenti automatizzati e nei casi di profilazione. Inoltre, è doveroso svolgere attività di impact assessment anche quando siamo in presenza di sorveglianza sistematica di una zona accessibile al pubblico su larga scala. Sotto quest'ultimo profilo, si pensi alla videosorveglianza in ambito pubblico. Ciascun Stato membro può chiedere in determinati casi che i Titolari del trattamento consultino l'Autorità Garante e ne ottengano una autorizzazione preliminare. All'Autorità Garante sono demandati compiti specifici in tema di individuazione di tipologie di trattamento da sottoporre a verifica di impatto privacy o, al contrario, da sottrarre. La valutazione di impatto sulla protezione dei dati deve contenere una descrizione del trattamento, con particolare attenzione alla finalità e all'interesse legittimo del Titolare al trattamento in parola, nonché una descrizione delle misure opportune e congrue a contrastare i rischi privacy.

Pertanto, le organizzazioni sia private che pubbliche non potranno più limitarsi a nominare un dipendente con il compito di "fare il minimo", ma dovranno approcciare la materia della tutela dei dati personali con una visione *corporate*, destinandovi sia fonti economiche adeguate, che personale competente.
Sotto quest'ultimo profilo, non possiamo esimerci dal citare la figura del ***data protection officer*** (art. 37), che diventa obbligatoria in tutta una serie di casistiche e che giocherà un ruolo fondamentale ai fini della responsabilità giuridica ascrivibile al titolare del trattamento, sotto il profilo della *culpa in eligendo* e in vigilando. Al riguardo si vedano le linee guida adottate dal Gruppo dei Garanti europei il 13 dicembre 2016 (WP 243).
Un preciso e puntuale *privacy impact assessment*, condotto da professionisti del settore (*data protection officer*), è un elemento fondamentale per l'attuazione di un'altra novità introdotta dal regolamento: la c.d. ***privacy by design e by default*** (art. 25).
La protezione dei dati fin dalla progettazione e con impostazioni predefinite sta a significare che qualsiasi progetto ad impatto privacy deve nascere ed essere costruito con impostazioni di default che rispettino la disciplina in tema di protezione dei dati personali. La norma ha un interessante collegamento con l'articolo 42 del Regolamento, secondo il quale è auspicabile che le Autorità Pubbliche incoraggino l'istituzione di meccanismi di certificazione della protezione dei dati, nonché di sigilli e marchi di protezione dei dati, allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento. In ogni caso, la certificazione non riduce la responsabilità del titolare (vedi il comma 4 dell'articolo 42), ma sarà in grado di influire sulla gravità delle sanzioni in ossequio al principio dell'*accountability*.
Privacy impact assessment ed il rispetto dei principi di *privacy by design e default* sono fondamentali per affrontare i casi di ***data brech notification,*** introdotti dall'art. 33 del nuovo regolamento.

Con l'introduzione della disciplina sulla notificazione di violazione dei dati personali, le Autorità Garanti dovranno essere informate tempestivamente dai Titolari dei casi di violazione dei dati personali (es. accesso illegittimo a banche dati o a sistemi informatici). Il titolare del trattamento, in caso di violazione dei dati personali, dovrà salvo casi particolari senza ingiustificato ritardo, e comunque entro 72 ore dal momento in cui ne è venuto a conoscenza, notificare la violazione al Garante.

Un'altra importante novità contenuta nel nuovo regolamento europeo riguarderà i grandi operatori del mondo on-line, che dovranno rispettare i principi europei, qualora intendano offrire i loro servizi in Europa. E' poi previsto un rafforzamento delle Autorità Garanti, le quali potranno fornire, attraverso linee guida ed altri strumenti, principi e metodologie al passo con l'inarrestabile sviluppo tecnologico, nell'auspicio che disciplinari tecnici come il noto Allegato "b", risalente al 2003 e mai aggiornato, rimangano un lontano retaggio del passato. Non da ultimo va citato il nuovo quadro sanzionatorio, caratterizzato da sanzioni che potranno arrivare sino al 4% del fatturato mondiale annuo della società, in caso di violazioni particolarmente gravi.
Per ulteriori approfondimenti si la guida applicativa recentemente emanata dal nostro Garante e pubblicata sul sito istituzionale (www.garanteprivacy.it)
La Guida traccia un quadro generale delle principali innovazioni introdotte dalla normativa e fornisce indicazioni utili sulle prassi da seguire e gli adempimenti da attuare per dare corretta applicazione alla normativa, già in vigore dal 24 maggio 2016 e che sarà pienamente efficace dal 25 maggio 2018.

Avv. Marco Soffientini
Studio Legale Rosadi Soffientini Associati

Proprietario ed editore:
Federazione ANIE
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.1
Direttore Responsabile
Maria Antonietta Portaluri
Registrazione del Tribunale
di Milano al n° 116 del
19/2/1996

***Te*Lex Anie**

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE
CONFINDUSTRIA

Pubblicazione a cura di:
Servizio Centrale Legale
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.246
e-mail legale@anie.it
Diffusione via web www.anie.it

Mini Master ANIE sulla Privacy: partecipa