TeLex Anie
NOVITÀ LEGISLATIVE E GIURISPRUDENZIALI
Estratto
N. 7/8 Anno XXII
Luglio/Agosto 2017

PRIVACY

DATA BREACH NOTIFICATION E PRIVACY IMPACT ASSESSMENT NEL NUOVO REGOLAMENTO UE 2016/679

Il 04 maggio 2016 è stato pubblicato, sulla Gazzetta Ufficiale dell'Unione europea, il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche e 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. Il 25 maggio 2016 il Regolamento è entrato in vigore dopo una *vacatio legis* di venti giorni, ma si applicherà a decorrere dal 25 maggio 2018 (articolo 99 Regolamento).

Gli aspetti di interesse per l'interprete, introdotti dal nuovo regolamento, sono molteplici. Si pensi al diritto all'oblio (art.17), al diritto alla portabilità dei dati (art. 20), al diritto di accesso (art. 15), al registro delle attività di trattamento (art. 30), alla Sicurezza del trattamento (art. 32), al meccanismo dello sportello unico (art. 60), alla disciplina su social e minori (art.8), al nuovo impianto sanzionatorio (art. 83), etc.
Ma gli architravi, su cui poggia tutto il sistema del nuovo regolamento e che sono alla base di una corretta configurazione di un sistema di gestione privacy, sono:

- il principio dell'accountability (art. 5, comma 2)
- la data protection impact assessment (art. 35)
- la data breach notification (art. 33)
- la privacy by design e by default (art. 25)

Soffermiamoci brevemente sugli istituti della data protection impact assessment e della data breach notification.

La valutazione d'impatto sulla protezione dei dati personali (**data protection impact assessment** *) è un istituto 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 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. La valutazione di impatto privacy è anche un'attività fondamentale e propedeutica nella progettazione di sistemi di gestione privacy conformi ai principi della **privacy by design e by default** (art. 25 Regolamento).

Una corretta progettazione di un sistema di gestione privacy è fondamentale per attenuare i danni derivanti da una data breach. Infatti, il regolamento introduce, in capo ai titolari del trattamento, un obbligo generalizzato di comunicazione delle violazioni di dati personali (**data breach notification**) **soltanto se ritengono probabile che da tale violazione derivino rischi** per i diritti e le libertà degli interessati. La ratio della disciplina si evince dal Considerando 85**:** *una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che,*

conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

La **data breach notification** è una procedura che il nostro ordinamento giuridico in materia di data protection già conosce in alcuni ambiti specifici. Si pensi al caso dei fornitori di servizi di comunicazione accessibili al pubblico (articoli 32 e 32 bis del Codice Privacy), su cui il Garante è intervenuto con il provvedimento 4 aprile 2013 (Pubblicato sulla Gazzetta Ufficiale n. 97 del 4 aprile 2013), doc. web n. 2388260 Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach). Si vedano anche le "Linee Guida in materia di dossier sanitario" (Provvedimento 4 Giugno 2015), dove i titolari di trattamento dei dati personali effettuati mediante il dossier sanitario sono tenuti a comunicare al Garante le violazioni dei dati personali (data breach) che si verificano nell'ambito delle proprie strutture. In ambito pubblico, il provvedimento 2 luglio 2015 "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche" doc. web n. 4129029 stabilisce, per le amministrazioni pubbliche, l'obbligo di comunicare al Garante le violazioni dei dati personali, che si verificano nell'ambito delle banche dati (qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, art. 4, comma 1, lett. p del Codice), di cui sono titolari. Infine, in tema di biometria, il Garante, con il Provvedimento 12 novembre 2014 (Provvedimento generale prescrittivo in tema di biometria), ha previsto il dovere in capo ai titolari di trattamento di dati biometrici di comunicare all'Autorità tutte le violazioni dei dati o gli incidenti informatici, che possano avere un impatto significativo sui sistemi biometrici o sui dati personali ivi custoditi.

Nota *****
Art. 35 Regolamento. Per maggiori approfondimenti si vedano le Linee Guida in tema di valutazione d'impatto privacy, rilasciate in data 04 aprile 2017 (WP 248) dal Gruppo dei Garanti Europei "Articolo 29" e la ISO/IEC 29134:2017 applicabile a qualsiasi organizzazione privata o pubblica.

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