diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 25/07/2016

All'indirizzo http://www.diritto.it/docs/38513-il-nuovo-regolamento-privacy-europeo-data-breach-e-data-portability

Autore: Marcoccio Gloria

Il nuovo regolamento privacy europeo: data breach e data portability

Nuovo regolamento privacy europeo GDPR: alcune considerazioni combinate in materia di Data Breach e Data Portability

Gloria Marcoccio - gloria.marcoccio@glory.it
23 Luglio 2016

Il nuovo regolamento privacy europeo n. 2016/679, già noto come GDPR (General Data Protection Regulation) ed entrato in vigore a fine Maggio di quest'anno, ha acceso un ampio dibattito ed ovviamente è oggetto di analisi ed approfondimenti che nel corso dei due anni che ci separano dalla sua applicabilità (a partire dal 5 maggio 2018) dovranno chiarire e supportare le implementazioni delle misure necessarie da parte di Titolari e Responsabili di trattamento dati, misure da avviare ed attuare proprio nel corso di questi due anni per poter essere pronti ed in regola con questa nuova legge dal momento in cui sarà applicabile (e dunque le inadempienze saranno sanzionabili).
Il regolamento è caratterizzato in particolare da un ambito territoriale assai ben più ampio del contesto dei paesi membri UE[1] e da prescrizioni nuove rispetto alla direttiva europea sulla privacy 95/46/EC, che richiedono nel loro complesso particolare attenzione anche tenendo presente il nuovo e consistente quadro sanzionatorio delineato dal GDPR[2].
Nelle analisi e negli approfondimenti occorre poi tener presenti le correlazioni ed interdipendenze che naturalmente esistono e legano tra loro alcune prescrizioni, così da poter stabilire ed applicare un metodo da seguire nell'implementare le misure necessarie per adempiere, che sia consistente e robusto, ma sempre in sintonia con le dimensioni ed il business della singola organizzazione, pubblica o privata, allo scopo di evitare costi e responsabilità aggiuntive, rischio sicuramente presente con maggior probabilità soprattutto per le piccole-medie imprese tenendo presente la gran quantità di obblighi e prescrizioni che caratterizzano il GDPR.
In questo articolo prendiamo in considerazione alcuni aspetti che riguardano le prescrizioni in materia di Violazione dei dati Personali (Data Breach) e la Portabilità dei dati (Data Portability) e le possibili loro relazioni ed interdipendenze da tenere presenti ai fini delle implementazioni delle necessarie misure.

Data Breach è in estrema sintesi l'obbligo che hanno i Titolari di comunicare al Garante privacy competente i casi di violazioni dati personali se queste presentano rischi per i diritti e le libertà delle persone fisiche (Art 33 GDPR). Se poi la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, allora il Titolare dovrà effettuare anche la comunicazione di avvenuta violazione dati personali agli Interessati (Art 34 GDPR). La comunicazione agli Interessati non è obbligatoria solo in casi particolari (esempio non esaustivo: se i dati sono sottoposti a misure di sicurezza quali la cifratura). Gli adempimenti in materia di Data Breach si applicano indipendentemente dal settore di attività e dalla dimensione del Titolare (pubblico o privato) che effettua il trattamento dati personali. Da notare che il Titolare del trattamento deve prendere anche decisioni (la violazione presenta effettivamente un rischio per le persone? e questi rischi sono anche tali da minare i diritti e le libertà delle persone?).
L'inadempienza può costare fino a 10 milioni di euro o 2% del fatturato mondiale (se superiore ai 10 milioni di euro).

Data Portability è uno dei nuovi importanti diritti sanciti dal GDPR (Art 20): l'Interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti ad un Titolare ed ha il diritto di trasmettere tali dati ad un altro Titolare senza impedimenti da parte del Titolare cui li ha precedentemente forniti se il trattamento, effettuato con mezzi automatizzati, si basa sul consenso o su un contratto con l'Interessato e se l'esercizio di questo diritto non

[1] Vedasi l'articolo pubblicato su www.diritto.it "European General Data Protection Regulation - Territorial Scope at a glance" : http://www.diritto.it/docs/38074-european-general-data-protection-regulation-territorial-scope-at-a-glance

[2] Vedasi l'articolo pubblicato su www.diritto.it "An overview about sanctions provided for by the new European Regulation on personal data protection" : http://www.diritto.it/docs/37782-an-overview-about-sanctions-provided-for-by-the-new-european-regulation-on-personal-data-protection

lede i diritti e le libertà altrui. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare.
L'Interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un Titolare del trattamento all'altro, se tecnicamente fattibile.
A puro titolo di esempio, non esaustivo, sono soggetti alle prescrizioni di Portability i servizi di email, social networking, data storing in cloud computing o meno, ma in teoria anche i dati che conserva un professionista al quale una persona fisica ha affidato un incarico.
L'inadempienza può costare fino a 20 milioni di euro o 4% del fatturato mondiale (se superiore ai 10 milioni di euro).

Qualche combinata considerazione

Dovremo dunque aspettarci che per un Titolare che subisce violazioni di dati personali nei suoi sistemi/servizi sia più probabile che un numero maggiore di Interessati richieda di avvalersi del diritto di Portabilità dei loro dati?
Questo evidentemente comporterà degli impatti negativi sul business per questi Titolari.
Alcuni Titolari potrebbero quindi essere portati a mascherare il più possibile i casi di violazione dati subiti? Potrebbero farlo ad esempio con un uso distorto dei processi decisionali che determinano o meno la notifica al Garante privacy competente e /o la comunicazione della violazione agli Interessati.
Oppure potrebbe instaurarsi un volano virtuoso per cui le aziende (Titolari, Responsabili) investiranno di più in misure di sicurezza appropriate quali la cifratura?
E come tutto questo potrà essere affrontato dai Titolari ricorrendo a servizi di assicurazione contro i cyber risk, servizi che sempre più spesso saranno disponibili sul mercato?
E gli Interessati come potranno effettivamente far valere il loro diritto alla portabilità dei dati?
Infatti dobbiamo riconoscere che un conto è parlare con un medio-piccolo Titolare nazionale, un conto è farlo con una multinazionale straniera rispetto la quale è evidente la assoluta mancanza di bilanciamento tra le parti.
Forse una maggior rappresentanza degli Interessati tramite apposite organizzazioni potrebbe dare un concreto contributo nel far valere il diritto alla Portability anche nei confronti delle multinazionali.
Sicuramente man mano e con il tempo verranno alla luce altre considerazioni, ma in ogni caso, si prospetta sempre più impegnativo il compito dei Garanti privacy e delle autorità giudiziarie che dovranno individuare e sanzionare in modo effettivo, proporzionato e dissuasivo i Titolari che volontariamente non osservano le prescrizioni in oggetto.

Di certo queste brevi considerazioni sulle prescrizioni in materia di Violazione dei dati personali e sul diritto degli Interessati alla Portabilità dei loro dati personali mettono in evidenza come anche il compito di Titolari e Responsabili non sia semplice nell'implementare ed attuare l'operatività delle misure necessarie per operare in modo conforme al nuovo regolamento privacy e richieda, di fatto oltre che per espressi obblighi (Art. 5 ed Art. 30 del GDPR), anche una effettiva capacità di controllo nel gestire e dimostrare il proprio stato di conformità[3].

[3] Vedasi a titolo di esempio GDPR Compliance Reporting: http://privacyblog.jimdo.com/privacy-manager-tools/gdpr-compliance-reporting/