Il Regolamento UE 24 Giugno 2013, n. 611 sulla notifica delle violazioni di dati personali ("*personal data breach*"): profili operativi e adempimenti organizzativi per i fornitori di servizi di comunicazione elettronica accessibili al pubblico.

di:
Prof. Avv. Alessandro del Ninno
Studio Legale Tonucci & Partners
adelninno@tonucci.com

Indice

---

§ 1. Introduzione

A partire dal 25 agosto 2013 sarà immediatamente applicabile negli ordinamenti giuridici degli Stati membri UE (e senza necessità di recepimento mediante atto normativo nazionale) il Regolamento UE n. 611/2013 della Commissione del 24 giugno 2013 sulle misure applicabili alla notifica delle violazioni di dati personali a norma della direttiva 2002/58/CE del Parlamento europeo e del Consiglio relativa alla vita privata e alle comunicazioni elettroniche.

Con il Regolamento in esame si perfeziona ulteriormente il quadro normativo relativo alla tematica cosiddetta del "*personal data breaches*" e rispetto alla quale i fornitori di servizi di comunicazione elettronica accessibili al pubblico sono tenuti ad adempimenti organizzativi, tecnici, gestionali e di comunicazione al Garante di non piccola entità.

Appare allora opportuno riepilogare sommariamente nella presente analisi il quadro di regole di riferimento, in un'ottica di coordinamento dei vari atti che hanno implementato le norme in materia di "*data breach*" e –

soprattutto – evidenziare gli elementi di novità che rispetto a tale quadro sono stati introdotti con il Regolamento UE 611/2013.

* * * *

§ 2. Il quadro delle norme in materia di "*personal data breach*"e la platea di soggetti destinatari degli obblighi di notifica.

Prima della adozione del Regolamento UE in esame, il quadro normativo ed amministrativo degli obblighi e adempimenti in materia di "violazione dei dati personali" era costituito:

- dall'art. 4 della direttiva 2002/58/Ce (c.d. direttiva e-Privacy) modificata dalla direttiva 2009/136/Ce;
- dal decreto legislativo 28 maggio 2012, n. 69, con il quale il Governo ha recepito le nuove norme di cui al punto precedente;
- dalla Decisione della Commissione UE sulle misure applicabili alla notifica di violazioni di dati personali ai sensi della Direttiva 2022/58/Ce;
- dal "*Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach)*" adottato dal Garante per la protezione dei dati personali in data 4 Aprile 2013.

In particolare, il decreto legislativo 28 Maggio 2012, n. 69, nell'ambito del recepimento delle direttive comunitarie sopra citate di aggiornamento e integrazione della riforma del quadro regolamentare delle comunicazioni elettroniche introdotto per la prima volta nel 2002, ha apportato specifiche modifiche e integrazioni al d.lgs. 30 Giugno 2003, n. 196 (Codice della privacy).

Sono state introdotte modifiche alle definizioni dell'art. 4 del Codice che sostituiscono o integrano i concetti giuridici di *chiamata*, *reti di comunicazione elettronica*, *rete pubblica di comunicazioni* in conformità alle definizioni già presenti nell'ordinamento comunitario.

E' altresì introdotta nel Codice della privacy la nuova definizione di "*violazione dei dati personali*", intesa come una "*violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico*".

Ancora, è stato modificato l'art. 32 del Codice sugli obblighi di sicurezza per i fornitori di servizi di comunicazione elettronica accessibili al pubblico (ora estesi anche ai diversi soggetti cui sia affidata l'erogazione

dei predetti servizi), ed è stato aggiunto il nuovo articolo 32-*bis* rubricato "*Adempimenti conseguenti ad una violazione di dati personali*", che prevede misure che includono l'obbligo per un fornitore dei servizi di comunicazione elettronica di segnalare al Garante privacy l'avvenuta violazione di dati personali e – nei casi di violazioni che rischino di pregiudicare tali dati o la riservatezza di un contraente o di un'altra persona - l'obbligo di comunicare la violazione direttamente anche a questi ultimi (tra l'altro, tali fornitori sono ora obbligati dal nuovo articolo 132-*bis* del Codice – come introdotto dal decreto – ad istituire apposite e specifiche procedure interne per corrispondere alle richieste di accesso a propri dati personali trasmesse dagli utenti, dovendo altresì fornire al Garante privacy – a richiesta - le informazioni su tali procedure, sul numero di richieste ricevute, sui motivi legali addotti e sulle risposte date).

Successivamente, all'esito di una consultazione pubblica, il Garante ha emanato le regole applicative in materia di notifica delle violazioni di dati personali mediante il *Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach)"* del 4 Aprile 2013. Con tale atto, l'Autorità per la protezione dei dati personali ha fornito linee guida operative e i modelli e format ufficiali per le notifiche dei casi di *data breach*.

Il quadro normativo e l'insieme di regole in materia di "*personal data breach*" si applicano ad una platea limitata di titolari del trattamento interessati: gli obblighi di comunicazione al Garante e alle persone interessate non riguardano infatti la totalità dei titolari dei trattamenti, ossia dei soggetti, pubblici o privati, che detengono e trattano dati personali in funzione della propria attività. I nuovi adempimenti gravano, infatti, esclusivamente sui "*fornitori di servizi di comunicazione elettronica accessibili al pubblico*" (es: compagnie telefoniche, Internet Service Providers, etc) e, quindi, su quei soggetti che mettono a disposizione del pubblico, su reti pubbliche di comunicazione, servizi consistenti, esclusivamente o prevalentemente, "nella trasmissione di segnali su reti di comunicazioni elettroniche" (art. 4, comma 2, lett. d) ed e), del Codice).

Il Garante ha chiarito nel Provvedimento del 4 Aprile 2013 che al contrario non rientrano tra tali soggetti:

- coloro che offrono direttamente servizi di comunicazione elettronica a gruppi delimitati di persone (come, a titolo esemplificativo, i soggetti pubblici o privati che consentono soltanto a propri dipendenti e collaboratori di effettuare comunicazioni telefoniche o telematiche). Tali servizi, pur rientrando nella definizione generale di "*servizi di comunicazione elettronica*", non possono essere infatti considerati come "*accessibili al pubblico*";

- i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie che si limitino a porre a disposizione del pubblico, di clienti o soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, ovvero punti di accesso a Internet utilizzando tecnologia wi-fi, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale;

- i gestori dei siti Internet che diffondono contenuti sulla rete (c.d. "*content provider*"). Essi non sono, infatti, fornitori di un "*servizio di comunicazione elettronica*" come definito dall'art. 4, comma 2, lett. e) del Codice. Tale norma, infatti, nel rinviare, per i casi di esclusione, all'art. 2, lett. c) della direttiva 2002/21/Ce cit., esclude essa stessa i "*servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica […]*". Qualora tali soggetti offrano anche il servizio di posta elettronica, limitatamente alla gestione dei dati personali relativi allo stesso, rientrano viceversa nel campo di applicazione della nuova disciplina;

- i gestori di motori di ricerca, salvo l'eventuale componente di trasmissione dati.

E' sempre il Garante a chiarire che invece rientra nell'ambito di applicabilità delle norme in esame la fornitura di servizi di *mobile payment* eventualmente offerti dal fornitore ai propri utenti. Si tratta di servizi che consentono di effettuare pagamenti o trasferimenti di denaro tramite telefono mobile, che molti fornitori stanno implementando a seguito del recepimento della direttiva n. 2007/64/Ce (la c.d. PSD, "*Payment Service Directive*") ad opera del d.lgs. 27 gennaio 2010, n. 11.

Più specificamente, osserva l'Autorità, il pagamento del bene o servizio acquistato avviene o mediante carta di credito su disposizione inviata per il tramite del telefono mobile in presenza di apposito lettore POS (c.d. modalità "*proximity*"), oppure con addebito e conseguente decurtazione del costo dal credito telefonico, per i clienti dotati di una carta ricaricabile, e con addebito sul conto telefonico, per i clienti in abbonamento (c.d. modalità "*remote*"). In quest'ultimo caso, i dati di pagamento dei clienti sono strettamente connessi a quelli di traffico telefonico degli stessi e pertanto il Garante ritiene che anche per le violazioni riguardanti tali servizi il fornitore sia tenuto agli obblighi di notifica di violazione dei dati personali.

L'Autorità specifica poi – sempre nel Provvedimento del 4 Aprile 2013 - che la nuova normativa prende espressamente in considerazione l'ipotesi in cui il fornitore affidi l'erogazione del servizio di comunicazione elettronica ad altri soggetti. In particolare, l'art. 32-*bis*, comma 8, prevede che, in questi casi, i soggetti esterni affidatari dell'erogazione del servizio

(es: i c.d. operatori virtuali di rete mobile - Mobile Virtual Network Operator, MVNO - ossia le società che forniscono servizi di telefonia mobile senza possedere alcuna licenza per il relativo spettro radio né tutte le infrastrutture necessarie) siano tenuti a comunicare senza indebito ritardo al fornitore (e cioè entro 24 ore, come specifica il Garante) tutti gli eventi e le informazioni necessarie a consentire a quest'ultimo di effettuare gli adempimenti in materia di violazione dei dati personali.

Formulando alcune conclusioni sull'ambito soggettivo di applicabilità delle regole in materia di notifica delle violazioni in materia di dati personali, ci si dovrebbe chiedere se l'interesse degli utenti ad essere informati sulle violazioni di sicurezza che coinvolgono i loro dati personali si limiti al settore delle comunicazioni elettroniche o non sia in realtà più ampio e generale. Ed infatti, proprio in tale prospettiva, lo schema di Regolamento UE di riforma della disciplina comunitaria sulla tutela dei dati personali (che sarà adottato all'inizio del 2014 per entrare a pieno regimo a partire dal 2016) già prevede un'estensione generalizzata dell'obbligo di notifica delle violazioni dei dati personali a tutti i titolari pubblici e privati, come peraltro già avviene in alcune legislazioni europee (es: in Irlanda) e come già auspicato dal Gruppo dei Garanti europei nel documento n. 01/2011, adottato il 5 aprile 2011.

* * * *

§ 3. Il Regolamento 611/2013: i nuovi contenuti ad integrazione del quadro normativo già vigente in materia di "*data breach*".

Cosa aggiunge dunque il nuovo Regolamento al già dettagliato quadro normativo sopra richiamato?

Intanto, occorre ricordare che per garantire l'attuazione uniforme delle misure di cui all'articolo 4, paragrafi 2, 3 e 4 della direttiva 2002/58/CE, l'articolo 4, paragrafo 5, della stessa direttiva conferisce alla Commissione la facoltà di adottare misure tecniche di attuazione riguardanti le circostanze, il formato e le procedure applicabili alle prescrizioni in materia di informazioni e comunicazioni di violazioni dei dati personali: l'esistenza difatti di requisiti nazionali divergenti in proposito potrebbe dar luogo a incertezza giuridica determinando procedure più complesse e gravose e costi amministrativi considerevoli per i fornitori che operano a livello transfrontaliero. In tale ottica va dunque inquadrato il Regolamento 611/2013 con il quale la Commissione ha appunto adottato le misure tecniche di attuazione degli obblighi in generale previsti dalla Direttiva 2002/58 come modificata dalla Direttiva 2009/136, specificando standard, procedure e format di comunicazione.

Il Regolamento riguarda poi esclusivamente la notifica delle violazioni di dati personali già verificatesi (la constatazione di una violazione di dati personali è considerata avvenuta se il fornitore ha acquisito elementi relativi a un incidente di sicurezza che ha compromesso dati personali sufficienti a giustificare una notifica) e non fissa pertanto misure tecniche di attuazione con riguardo agli obblighi di informazione degli abbonati nel caso in cui esista un particolare rischio di violazione della sicurezza della rete.

In realtà, molte delle previsioni contenute nel Regolamento sono state già implementate nell'ordinamento, soprattutto avuto riguardo all'assai dettagliato Provvedimento Generale del Garante del 4 Aprile 2013 (che specifica anche i termini temporali – di 24 ore o di tre giorni a seconda dei vari casi – entro i quali procedere alle notifiche).

Appare allora opportuno evidenziare i soli contenuti del Regolamenti 611/2013 fino ad ora non previsti nel quadro normativo e attuativo di riferimento e dunque integrativi degli obblighi di notifica di "*personal data breach*".

Un primo contenuto "nuovo" introdotto dal Regolamento 611/613 riguarda il chiarimento di cui all'art. 2, comma 1: "*Il fornitore notifica all'autorità nazionale competente tutte le violazioni di dati personali*". I fornitori sono tenuti cioè a notificare tutte le violazioni di dati personali e pertanto ad essi non è lasciata alcuna possibilità di decidere se informare o meno l'Autorità di protezione dei dati personali (la quale resta libera di adottare le misure necessarie per evitare che vi siano troppe o troppo poche notifiche di violazioni di dati personali).

Un secondo elemento di novità riguarda poi i casi di violazione che rischiano di pregiudicare i dati personali o la vita privata di un abbonato o di altra persona interessata e che implicano l'obbligo - in aggiunta alla notifica all'Autorità nazionale – di comunicare l'avvenuta violazione anche all'abbonato o all'altra persona. In tale prospettiva il Garante per la privacy nel Provvedimento del 4 aprile 2013 aveva già indicato ai fornitori di servizi di comunicazione elettronica alcuni criteri per decidere se comunicare o meno al contraente o ad altre persone interessate l'avvenuta violazione dei loro dati personali. Il Regolamento 611/2013 codifica ora i casi di violazione rispetto ai quali scatta l'obbligo di comunicazione all'abbonato o ad altra persona.

L'art. 3 dispone difatti che l'eventualità che una violazione di dati personali possa pregiudicare i dati personali o la vita privata di un abbonato o di un'altra persona è valutata dai fornitori tenendo conto, in particola-

re, delle seguenti circostanze (ovviamente non esaustive, ma comunque chiarificatrici):

a) la natura e il contenuto dei dati personali interessati, in particolare qualora essi riguardino informazioni finanziarie, categorie particolari di dati (come ad esempio i dati sensibili o biometrici) nonché dati relativi all'ubicazione, file di connessione a Internet, cronologie di navigazione in rete, dati relativi alla posta elettronica ed elenchi dettagliati delle chiamate;
b) le probabili conseguenze della violazione di dati personali per l'abbonato o l'altra persona interessata, in particolare nel caso in cui la violazione possa comportare furto o usurpazione di identità, danni fisici, disagio psicologico, umiliazione o danni alla reputazione; nonché
c) le circostanze della violazione di dati personali, in particolare nel caso in cui i dati siano stati rubati o se il fornitore è a conoscenza del fatto che i dati sono in possesso di un terzo non autorizzato.

Altro elemento innovativo è il divieto ai fornitori di sfruttare l'obbligo di notifica al contraente o ad altra persona (magari non cliente del fornitore) per farne occasione di *marketing* …: dispone infatti l'art. 3, comma 4 del Regolamento che "*la notifica all'abbonato o all'altra persona è espressa in modo chiaro e facilmente comprensibile. Il fornitore non si serve della notifica come mezzo per promuovere o pubblicizzare servizi nuovi o aggiuntivi*".

Al Regolamento sono poi acclusi due Allegati. L'Allegato I ("*Contenuto della notifica all'autorità nazionale competente*") prescrive il contenuto obbligatorio della notifica di violazione dei dati personali che il fornitore di servizi di comunicazione elettronica deve trasmettere elettronicamente e in via telematica all'autorità nazionale di protezione dei dati. Tale Allegato I del Regolamento è già per intero implementato dal "*Modello di segnalazione di data breach*" allegato al Provvedimento del Garante privacy del 4 aprile 2013: anzi, rispetto alle 17 indicazioni da fornire come evidenziate dall'Allegato I del Regolamento, il Modello del Garante ne richiede circa 60.

Innovativo è invece l'Allegato II al Regolamento ("*Contenuto della notifica all'abbonato o ad altra persona*") che prescrive il contenuto della comunicazione che il fornitore di servizi di comunicazione elettronica – ricorrendone i presupposti - deve trasmettere al contraente o ad altre persone i cui dati personali siano stati interessati dalla avvenuta violazione. Fino ad ora non erano state codificate le informazioni obbligatorie di base da comunicare al contraente o ad altra persona interessata nel caso di violazioni dei loro dati personali: lo stesso Garante nel Provvedimento del 4 aprile 2013 ha fatto mero riferimento a quanto prescritto dal comma 5 dell'art. 32-

bis del Codice della privacy ("*la comunicazione al contraente o ad altra persona contiene almeno una descrizione della natura della violazione di dati personali e i punti di contatto presso cui si possono ottenere maggiori informazioni ed elenca le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione di dati personali*"). Con l'Allegato II al Regolamento 611/2013 si specifica invece quali sono le informazioni da fornire al contraente o ad altra persona interessata dal "*data breach*":

1. Nome del fornitore
2. Identità e coordinate di contatto del responsabile della protezione dei dati o di un altro referente presso cui ottenere maggiori informazioni
3. Sintesi dell'incidente che ha provocato la violazione di dati personali;
4. Data presunta dell'incidente
5. Natura e contenuto dei dati personali in questione;
6. Probabili conseguenze della violazione dei dati personali per un abbonato o altra persona interessata;
7. Circostanze della violazione di dati personali in questione;
8. Misure adottate dal fornitore per rimediare alla violazione di dati personali
9. Misure consigliate dal fornitore per attenuare i possibili effetti negativi.

* * * * *