REGOLAMENTI

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

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

vista la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) ([1]), in particolare l'articolo 4, paragrafo 5,

previa consultazione dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA),

previa consultazione del gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'articolo 29 della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ([2]) (il gruppo dell'articolo 29),

previa consultazione del Garante europeo della protezione dei dati (GEPD),

considerando quanto segue:

(1) La direttiva 2002/58/CE prevede l'armonizzazione delle disposizioni nazionali necessarie per garantire un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata e alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno dell'Unione.

(2) A norma dell'articolo 4 della direttiva 2002/58/CE, i fornitori di servizi di comunicazione elettronica accessibili al pubblico sono tenuti a notificare le violazioni di dati personali alle autorità nazionali competenti e, in alcuni casi, anche agli abbonati e alle altre persone interessate. Ai sensi dell'articolo 2, lettera i), della direttiva 2002/58/CE, si intende per «violazione dei dati personali» una violazione di sicurezza che comporta accidentalmente o in modo illecito 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 nell'Unione.

(3) 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 cui allo stesso articolo.

(4) L'esistenza di requisiti nazionali divergenti in proposito può dar luogo a incertezza giuridica, a procedure più complesse e gravose e a costi amministrativi considerevoli per i fornitori che operano a livello transfrontaliero. La Commissione ritiene pertanto necessario adottare le suddette misure tecniche di attuazione.

(5) Il presente regolamento riguarda esclusivamente la notifica delle violazioni di dati personali e non fissa pertanto misure tecniche di attuazione con riguardo all'articolo 4, paragrafo 2, della direttiva 2002/58/CE sull'informazione degli abbonati nel caso in cui esista un particolare rischio di violazione della sicurezza della rete.

(6) Dall'articolo 4, paragrafo 3, primo comma, della direttiva 2002/58/CE consegue che i fornitori sono tenuti a notificare tutte le violazioni di dati personali all'autorità nazionale competente. Al fornitore non dev'essere pertanto lasciata la possibilità di decidere se informare o meno tale autorità. Ciò non deve tuttavia impedire all'autorità nazionale competente interessata di indagare in via prioritaria su determinate violazioni nel modo che ritiene adeguato conformemente alla legislazione applicabile e di adottare le misure necessarie per evitare che vi siano troppe o troppo poche violazioni di dati personali segnalate.

(7) È opportuno prevedere un sistema di notifica delle violazioni di dati personali all'autorità nazionale competente che comporti, ove sussistano determinate condizioni, fasi distinte a cui si applicano scadenze ben definite. Questo sistema è volto a garantire che l'autorità nazionale competente venga informata con la massima tempestività e precisione, senza tuttavia ostacolare indebitamente gli sforzi compiuti dal fornitore per indagare sulla violazione e prendere le misure necessarie per arginarla e porre rimedio alle sue conseguenze.

([1]) GU L 201 del 31.7.2002, pag. 37.
([2]) GU L 281 del 23.11.1995, pag. 31.

(8) Ai fini del presente regolamento, il semplice sospetto che si sia verificata una violazione di dati personali o la semplice individuazione di un incidente non accompagnati da informazioni sufficienti, malgrado tutti gli sforzi messi in atto da un fornitore per disporne, non possono essere considerati sufficienti per ritenere che è stata individuata una violazione di dati personali. A questo proposito, una particolare attenzione deve essere riservata al possesso delle informazioni di cui all'allegato I.

(9) Nel quadro dell'applicazione del presente regolamento, è opportuno che le autorità nazionali competenti interessate prestino la loro collaborazione nei casi di violazione di dati personali che presentano una dimensione transnazionale.

(10) Il presente regolamento non fornisce specifiche supplementari con riguardo all'inventario delle violazioni di dati personali che i fornitori devono compilare, dato che l'articolo 4 della direttiva 2002/58/CE ne definisce il contenuto in maniera esaustiva. I fornitori possono tuttavia far riferimento al presente regolamento per determinare il formato dell'inventario.

(11) È necessario che tutte le autorità nazionali competenti mettano a disposizione dei fornitori uno strumento elettronico sicuro per la notifica delle violazioni di dati personali in un formato comune, basato su una norma come l'XML e contenente le informazioni di cui all'allegato I nelle lingue pertinenti, in modo da consentire a tutti i fornitori all'interno dell'Unione di seguire una procedura di notifica analoga, a prescindere dal luogo di stabilimento e dal luogo della violazione. A questo proposito, è opportuno che la Commissione faciliti l'introduzione dello strumento elettronico sicuro organizzando, ove necessario, riunioni con le autorità nazionali competenti.

(12) Nel valutare se una violazione di dati personali rischia di pregiudicare i dati personali o la vita privata di un abbonato o di altra persona occorre tener conto, in particolare, della natura e del contenuto dei dati personali interessati, soprattutto nel caso di dati relativi a informazioni finanziarie quali numeri di carte di credito e coordinate bancarie, di categorie particolari di dati di cui all'articolo 8, paragrafo 1, della direttiva 95/46/CE nonché di alcuni dati specificamente legati alla fornitura di servizi di telefonia o Internet, ossia dati relativi alla posta elettronica, dati relativi all'ubicazione, file di connessione a Internet, cronologie di navigazione in rete ed elenchi dettagliati delle chiamate.

(13) In circostanze eccezionali è opportuno che il fornitore sia autorizzato a ritardare la notifica all'abbonato o ad altra persona, qualora tale notifica possa mettere a rischio il corretto svolgimento dell'indagine sulla violazione di dati personali. In questo contesto, le circostanze eccezionali possono includere indagini penali e altre violazioni di dati personali non equiparabili a un reato grave, ma per le quali può essere opportuno posticipare la notifica. È comunque opportuno che spetti alle autorità nazionali competenti valutare, caso per caso e alla luce delle circostanze, se accogliere il rinvio o esigere la notifica.

(14) I fornitori devono disporre delle coordinate dei propri abbonati, dato il loro rapporto contrattuale diretto, ma è possibile che tali informazioni non esistano per altre persone lese dalla violazione di dati personali. In tal caso, è opportuno che al fornitore venga consentito di informare in un primo tempo tali persone mediante annunci pubblicitari sui principali mezzi di comunicazione nazionali o regionali, come i giornali, per poi trasmettere, non appena possibile, una notifica individuale secondo quanto previsto dal presente regolamento. Il fornitore non è dunque espressamente obbligato a ricorrere a tali mezzi di comunicazione, ma ha piuttosto la facoltà di farlo se lo desidera, quando è ancora nella fase di identificazione di tutte le persone lese.

(15) È opportuno che le informazioni relative alla violazione si limitino esclusivamente alla violazione stessa e non siano associate ad informazioni di altro tipo. Ad esempio, l'inclusione di informazioni riguardanti una violazione di dati personali in una regolare fattura non può essere considerata un mezzo adeguato di notifica di tale violazione.

(16) Il presente regolamento non definisce misure tecnologiche di protezione specifiche che giustifichino una deroga all'obbligo di notifica delle violazioni di dati personali agli abbonati o ad altre persone interessate, poiché tali misure possono mutare nel tempo in funzione del progresso tecnologico. È tuttavia opportuno che la Commissione abbia la possibilità di pubblicare un elenco indicativo di tali misure tecnologiche di protezione specifiche in base alle prassi attuali.

(17) Il ricorso a tecniche di crittografia o di hashing non deve essere ritenuto di per sé sufficiente dai fornitori per poter asserire in termini più generali di aver ottemperato all'obbligo generale di sicurezza di cui all'articolo 17 della direttiva 95/46/CE. A tal riguardo, i fornitori devono altresì applicare adeguate misure organizzative e tecniche volte a prevenire, individuare e bloccare le violazioni di dati personali. Essi devono inoltre esaminare ogni rischio residuo ancora presente una volta applicati i controlli al fine di comprendere se sussiste la possibilità che si verifichino violazioni di dati personali.

(18) Se il fornitore ricorre a un altro fornitore per svolgere una parte del servizio, ad esempio per quanto riguarda la fatturazione o per funzioni di gestione, è opportuno che

quest'altro fornitore, che non ha un rapporto contrattuale diretto con l'utilizzatore finale, non sia obbligato a notificare le violazioni di dati personali. Esso deve invece allertare e informare il fornitore con cui ha un rapporto contrattuale diretto. Questo principio deve valere anche nel contesto della fornitura all'ingrosso di servizi di comunicazione elettronica, in cui in genere il fornitore all'ingrosso non ha un rapporto contrattuale diretto con l'utilizzatore finale.

(19) La direttiva 95/46/CE definisce un quadro generale per la protezione dei dati personali nell'Unione europea. La Commissione ha presentato una proposta di regolamento del Parlamento europeo e del Consiglio (il «regolamento sulla protezione dei dati») volto a sostituire la direttiva 95/46/CE. Il proposto regolamento sulla protezione dei dati intende introdurre l'obbligo per tutti i responsabili del trattamento di dati di notificare le violazioni di dati personali, sulla base dell'articolo 4, paragrafo 3, della direttiva 2002/58/CE. Il presente regolamento della Commissione è pienamente compatibile con la misura proposta.

(20) Il proposto regolamento sulla protezione dei dati introduce inoltre un numero limitato di adeguamenti tecnici alla direttiva 2002/58/CE per tener conto della conversione in regolamento della direttiva 95/46/CE. Le conseguenze in materia di diritto sostanziale per la direttiva 2002/58/CE prodotte dal nuovo regolamento saranno oggetto di una revisione della Commissione.

(21) È opportuno che l'applicazione del presente regolamento venga riesaminata a distanza di tre anni dall'entrata in vigore e che il suo contenuto sia riveduto alla luce del contesto giuridico in vigore in quel momento, incluso il proposto regolamento sulla protezione dei dati. Ove possibile, il riesame del presente regolamento deve essere associato a ogni futura revisione della direttiva 2002/58/CE.

(22) L'applicazione del presente regolamento può essere valutata fra l'altro in base alle statistiche tenute dalle autorità nazionali competenti con riguardo alle violazioni di dati personali che vengono loro notificate. Tali statistiche possono ad esempio includere informazioni sul numero di violazioni di dati personali notificate all'autorità nazionale competente, sul numero di violazioni di dati personali notificate all'abbonato o ad altra persona, sul tempo impiegato per rimediare alla violazione e sull'eventuale adozione di misure tecnologiche di protezione. È opportuno che tali statistiche forniscano alla Commissione e agli Stati membri dati statistici coerenti e comparabili senza rivelare né l'identità del fornitore da cui è partita la notifica né quella degli abbonati o delle altre persone coinvolte. A tal fine la Commissione può anche organizzare riunioni regolari con le autorità nazionali competenti e altre parti interessate.

(23) Le misure di cui al presente regolamento sono conformi al parere del comitato per le comunicazioni,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Campo di applicazione

Il presente regolamento si applica alla notifica delle violazioni di dati personali da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico («il fornitore»).

Articolo 2

Notifica all'autorità nazionale competente

1. Il fornitore notifica all'autorità nazionale competente tutte le violazioni di dati personali.

2. Il fornitore notifica all'autorità nazionale competente la violazione di dati personali entro un termine di 24 ore a partire dal rilevamento della violazione, ove possibile.

Il fornitore include nella propria notifica all'autorità nazionale competente le informazioni di cui all'allegato I.

La constatazione di una violazione di dati personali è considerata avvenuta se il fornitore ha acquisito elementi sufficienti, relativi a un incidente di sicurezza che ha compromesso dati personali, a giustificare una notifica a norma del presente regolamento.

3. Qualora le informazioni di cui all'allegato I non siano interamente disponibili e occorrano ulteriori indagini sulla violazione di dati personali, il fornitore è autorizzato a trasmettere all'autorità nazionale competente una notifica iniziale entro 24 ore a partire dal rilevamento della violazione. Questa notifica iniziale all'autorità nazionale competente contiene le informazioni di cui alla sezione 1 dell'allegato I. Non appena possibile, e al massimo entro tre giorni dalla notifica iniziale, il fornitore trasmette all'autorità nazionale competente una seconda notifica. Questa seconda notifica contiene le informazioni di cui alla sezione 2 dello stesso allegato e, se necessario, aggiorna le informazioni già fornite.

Il fornitore che, malgrado le indagini effettuate, non sia in grado di fornire tutte le informazioni entro tre giorni dalla notifica iniziale, notifica tutte le informazioni di cui dispone entro tale termine e presenta all'autorità nazionale competente una giustificazione motivata per la notifica tardiva delle informazioni residue. Non appena possibile, il fornitore notifica all'autorità nazionale competente tali informazioni residue e, se necessario, aggiorna le informazioni già fornite.

4. L'autorità nazionale competente mette a disposizione di tutti i fornitori stabiliti nello Stato membro interessato uno strumento elettronico sicuro per la notifica delle violazioni di dati personali nonché informazioni sulle procedure di accesso e di uso di tale strumento. Se necessario, la Commissione organizza riunioni con le autorità nazionali competenti per facilitare l'applicazione della presente disposizione.

5. Quando la violazione di dati personali riguarda abbonati o altre persone provenienti da uno Stato membro diverso da quello dell'autorità nazionale competente a cui la violazione di dati personali è stata notificata, l'autorità nazionale competente ne informa le altre autorità nazionali interessate.

Per facilitare l'applicazione della presente disposizione, la Commissione redige e mantiene aggiornato un elenco delle autorità nazionali competenti e di punti di contatto adeguati.

Articolo 3

Notifica all'abbonato o ad altra persona

1. Quando la violazione di dati personali rischia di pregiudicare i dati personali o la vita privata di un abbonato o di altra persona, in aggiunta alla notifica di cui all'articolo 2 il fornitore comunica l'avvenuta violazione anche all'abbonato o all'altra persona.

2. 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 tenendo conto, in particolare, delle seguenti circostanze:

a) la natura e il contenuto dei dati personali interessati, in particolare qualora essi riguardino informazioni finanziarie, categorie particolari di dati di cui all'articolo 8, paragrafo 1, della direttiva 95/46/CE, 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.

3. La notifica all'abbonato o all'altra persona è effettuata senza indebito ritardo dopo la scoperta della violazione di dati personali, secondo quanto previsto all'articolo 2, paragrafo 2, terzo comma. Tale notifica è indipendente dalla notifica della violazione di dati personali all'autorità nazionale competente, di cui all'articolo 2.

4. Il fornitore include nella propria notifica all'abbonato o altra persona interessata le informazioni di cui all'allegato II. 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.

5. In circostanze eccezionali, qualora la notifica all'abbonato o all'altra persona possa mettere a rischio il corretto svolgimento dell'indagine sulla violazione di dati personali, il fornitore è autorizzato, previo accordo dell'autorità nazionale competente, a ritardare la notifica all'abbonato o all'altra persona fino a quando la suddetta autorità ritenga possibile notificare la violazione di dati personali conformemente al presente articolo.

6. Il fornitore notifica all'abbonato o all'altra persona la violazione di dati personali facendo ricorso a mezzi di comunicazione che consentano un rapido recapito delle informazioni e la cui sicurezza sia garantita con le tecnologie più avanzate. Le informazioni relative alla violazione si limitano alla violazione stessa e non sono associate ad informazioni di altro tipo.

7. Il fornitore legato da un rapporto contrattuale diretto all'utilizzatore finale che, malgrado i ragionevoli sforzi profusi, non sia in grado di individuare entro il termine di cui al paragrafo 3 tutte le persone che potrebbero essere lese dalla violazione di dati personali, può informare tali persone entro lo stesso termine attraverso annunci pubblicitari nei principali mezzi di comunicazione nazionali o regionali negli Stati membri interessati. Tali annunci sono corredati delle informazioni riportate nell'allegato II, se necessario in forma sintetica. In tal caso, il fornitore continua a compiere tutti gli sforzi ragionevoli per identificare tali persone e notificare loro quanto prima le informazioni di cui all'allegato II.

Articolo 4

Misure tecnologiche di protezione

1. In deroga all'articolo 3, paragrafo 1, non è richiesta la notifica di una violazione dei dati personali a un abbonato o ad altra persona interessata se il fornitore ha dimostrato in modo convincente all'autorità nazionale competente di avere utilizzato adeguate misure tecnologiche di protezione e che tali misure erano state applicate ai dati interessati dalla violazione della sicurezza. Tali misure tecnologiche di protezione rendono i dati incomprensibili a chiunque non sia autorizzato ad accedervi.

2. I dati sono considerati incomprensibili se:

a) sono stati crittografati in modo sicuro mediante un algoritmo standardizzato, la chiave utilizzata per decifrarli non è stata compromessa nell'ambito di una violazione della sicurezza ed è stata generata in modo tale da non poter essere individuata con i mezzi tecnologici disponibili da qualcuno che non sia autorizzato ad accedervi; o

b) sono stati sostituiti dal loro valore hash calcolato mediante una funzione di hash con chiave crittografica normalizzata, la chiave utilizzata per l'hashing dei dati non è stata compromessa nell'ambito di una violazione della sicurezza ed è stata generata in modo tale da non poter essere individuata con i mezzi tecnologici disponibili da qualcuno che non sia autorizzato ad accedervi.

3. La Commissione, dopo aver consultato le autorità nazionali competenti tramite il gruppo dell'articolo 29, l'Agenzia europea per la sicurezza delle reti e dell'informazione e il Garante europeo della protezione dei dati, può pubblicare un elenco indicativo delle misure tecnologiche di protezione adeguate di cui al paragrafo 1, in base alle prassi attuali.

Articolo 5

Ricorso a un altro fornitore

Qualora per poter fornire una parte dei servizi di comunicazione elettronica si faccia ricorso a un altro fornitore che non ha un legame contrattuale diretto con gli abbonati, questo altro fornitore informa immediatamente il fornitore che lo ha ingaggiato in caso di violazione di dati personali.

Articolo 6

Relazioni e riesame

Entro tre anni dall'entrata in vigore del presente regolamento, la Commissione redige una relazione sull'applicazione del regolamento, la sua efficacia e il suo impatto sui fornitori, sugli abbonati e sulle altre persone. Sulla base di tale relazione la Commissione procede al riesame del presente regolamento.

Articolo 7

Entrata in vigore

Il presente regolamento entra in vigore il 25 agosto 2013.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 24 giugno 2013

Per la Commissione
Il presidente
José Manuel BARROSO

ALLEGATO I

Contenuto della notifica all'autorità nazionale competente

Sezione 1

Identificazione del fornitore

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. Indicare se si tratta di una prima o di una seconda notifica

Informazioni iniziali sulla violazione di dati personali (da compilare, ove del caso, nelle notifiche successive)

4. Data e ora dell'incidente (se note; ove necessario, può essere fornita una stima) e della constatazione dell'incidente
5. Circostanze della violazione di dati personali (ad esempio perdita, furto, copia)
6. Natura e contenuto dei dati personali in questione
7. Misure tecniche e organizzative che il fornitore ha applicato (o applicherà) ai dati personali violati
8. Ricorso giustificato ad altri fornitori (ove applicabile)

Sezione 2

Ulteriori informazioni circa la violazione dei dati personali

9. Sintesi dell'incidente che ha provocato la violazione di dati personali (inclusi il luogo fisico della violazione e il supporto di memorizzazione interessato)
10. Numero di abbonati o persone interessate
11. Potenziali conseguenze e potenziali effetti negativi per gli abbonati o altre persone
12. Misure tecniche e organizzative adottate dal fornitore per attenuare i potenziali effetti negativi

Eventuali ulteriori comunicazioni agli abbonati o ad altre persone

13. Contenuto della notifica
14. Mezzi di comunicazione utilizzati
15. Numero di abbonati o persone informate

Eventuali questioni transfrontaliere

16. Violazione di dati personali che riguardano abbonati o persone in altri Stati membri
17. Notifica ad altre autorità nazionali competenti

ALLEGATO II

Contenuto della notifica all'abbonato o ad altra persona

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, a norma dell'articolo 3, paragrafo 2

6. Probabili conseguenze della violazione dei dati personali per un abbonato o altra persona interessata, a norma dell'articolo 3, paragrafo 2

7. Circostanze della violazione di dati personali in questione, a norma dell'articolo 3, paragrafo 2

8. Misure adottate dal fornitore per rimediare alla violazione di dati personali

9. Misure consigliate dal fornitore per attenuare i possibili effetti negativi