

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.

