PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4295 di Lunedì 27 agosto 2018

La notifica di una violazione di dati prevista dal GDPR

L'articolo 33 del regolamento generale europeo impone che una violazione dei dati sia sempre notificata all'autorità Garante nazionale. Vi sono tuttavia eccezioni, debitamente illustrate da un documento dell'articolo 29 Working party.

Prima dell'entrata in vigore del regolamento generale europeo, l'autorità Garante nazionale richiedeva che venisse segnalata una violazione dei dati, solo quando tale violazione comportava dati biometrici, dati relativi al traffico telefonico e dati sanitari.

Il nuovo regolamento invece impone una generalizzata notifica all'autorità Garante nazionale, a fronte di una violazione di dati, sia di natura dolosa, sia di natura accidentale.

Occorre tuttavia leggere con molta attenzione l'articolo 33, perché la notifica non è necessaria, ove "sia improbabile che la violazione dei dati personali presenti per un rischio per i diritti e le libertà delle persone fisiche coinvolte."

Appare evidente che, non appena pubblicato il regolamento, da più parti venissero avanzate delle perplessità sulla corretta interpretazione di questa esenzione di notifica. A fronte di varie interpretazioni, l'articolo 29 Working party, sempre prezioso elemento di guida all'interpretazione del regolamento europeo, ha pubblicato un documento, che analizza in dettaglio questi scenari e dà precise indicazioni sulle circostanze nelle quali sia o meno necessaria la notifica.

Il documento in questione, contrassegnata dal codice wp251, rappresenta pertanto una preziosa guida per tutti i titolari e responsabile del trattamento, circa le circostanze nelle quali la notifica, che comunque deve essere presentata entro 72 ore dalla presa di conoscenza della violazione stessa, deve essere presentata o meno.

Il documento in questione è accompagnato da una preziosissima tabella, che illustra alcune esemplificazioni, nelle quali possa essere obbligatoria o meno la notifica.

Ad esempio, uno dei casi che più spesso può verificarsi e che maggiormente preoccupa i titolari, fa riferimento alla perdita di una chiavetta di memoria USB, sulla quale siano archiviati dati personali di interessati, trattati dal titolare.

Il documento mette chiaramente in evidenza che, ove tali dati siano stati archiviati sulla chiavetta con protezione criptografica, la notifica non deve essere presentata.

Ancora una volta, ricordo a tutti i lettori che l'utilizzo allargato di tecniche di protezione criptografica rappresenta uno strumento di protezione dei dati personali, di costo ridotto e di efficacia straordinaria. Ancora oggi, non riesco a comprendere il motivo per cui i titolari e responsabili coinvolti non utilizzino su larga scala questa tecnica di protezione, il cui costo e la cui efficacia sono incomparabili, rispetto ad altre soluzioni.

Nel rimandare i lettori all'attenta lettura del documento in questione, riporto in allegato una sintetica tabella, che illustra appunto alcune classiche situazioni di perdita dei dati, che possono meno portare alla attivazione o meno delle procedure di notifica.

Allegato tabella riepilogativa (doc)

Adalberto Biasiotti