PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4147 di Giovedì 21 dicembre 2017

La gestione di una violazione dei dati secondo il regolamento europeo

Il 3 ottobre 2017 l'articolo 29 working party ha pubblicato un documento di approfondimento sulle modalità di notifica di una violazione dei dati. Una lettura obbligatoria per chiunque abbia responsabilità connesse alla protezione dei dati personali.

Innanzitutto è bene ricordare che già numerosi Stati europei Italia compresa, hanno delle regole in materia di notificazione delle violazioni dei dati. La differenza fondamentale, che viene messa in evidenza nello studio del *working party 29* è legata al fatto che nel nuovo regolamento questo obbligo di notificazione è generalizzato.

Appare evidente che una perdita di dati è spesso conseguenza di una insoddisfacente gestione dei dati stessi, anche se è bene chiarire innanzitutto che cosa significhi perdita di dati personali.

È bene precisare che se una violazione dei dati rappresenta un incidente afferente alla sicurezza, questa perdita è rilevate solo se sono coinvolti dei dati personali.

La violazione può assumere diverse caratteristiche, come ad esempio:

- una violazione di riservatezza,

- una violazione di disponibilità,

- una violazione di integrità.

Ovviamente sono anche possibili combinazioni delle tre tipologie illustrate.

L'articolo 29 working party concentra la sua attenzione su una violazione afferente alla disponibilità, che si manifesta quando vi è una perdita o distruzione permanente di dati personali.

Se invece la perdita ha carattere temporaneo, l'obbligo di notificazione si potrebbe manifestare quando la durata della indisponibilità è tale da compromettere un regolare accesso ai dati, soprattutto per soddisfare, ad esempio, una richiesta di accesso da parte di un interessato. Un tipico esempio è una temporanea impossibilità di accesso perché il sistema informativo è stato colpito da un ransomware. In questo caso è sufficiente pagare il riscatto richiesto dai criminali per avere pronto accesso ai dati stessi.

Un altro aspetto interessante riguarda il fatto che la notificazione deve essere fatta quando il titolare del trattamento si rende conto che è avvenuta una violazione. Il documento elaborato dall'articolo 29 working party offre alcuni esempi che mettono in evidenza le circostanze, che possono determinare il momento in cui il titolare si è accorto della violazione. L'ora ed il giorno in cui il titolare si è accorto della violazione sono importanti, perché da quel momento decorrono i tempi per poter segnalare all'autorità Garante la violazione in corso.

Si tratta di un argomento importante, perché la violazione potrebbe avvenire presso enti terzi, cui il titolare ha conferito l'autorità di elaborare i dati; in questo caso questi enti terzi debbono immediatamente avvertire il titolare, in caso di violazione. È quindi opportuno che in un contratto di trattamento di dati siano inserite clausole specifiche su questo critico argomento.

Il documento passa quindi ad illustrare le modalità con cui deve essere inviata la notificazione all'autorità Garante con alcuni chiarissimi esempi.

Vengono anche chiarite le circostanze nelle quali non è necessario che la notificazione venga inviata anche gli interessati coinvolti. Quest'ultimo argomento è evidentemente particolarmente delicato ed occorre quindi chiarire bene quando l'interessato può o deve essere coinvolto. La comunicazione, se appropriata, deve essere fatta in un linguaggio oltre modo chiaro e, se del caso, deve essere concordata con l'autorità Garante nazionale ed anche con la Procura della Repubblica, se la violazione ha avuto carattere criminoso. La notificazione agli interessati deve essere tanto più completa ed articolata, quanto maggiore è il rischio connesso alla perdita di dati in esame.

Il documento si conclude con alcuni esempi pratici, oltremodo utili, che possono guidare il titolare in una corretta gestione di una violazione dei dati, sia essa accidentale, sia essa criminosa.

Adalberto Biasiotti

Scarica il documento da cui è tratto l'articolo:

Article 29 Data Protection Working Party- Guidelines on Personal data breach notification under Regulation 2016/679 - Adopted on 3 October 2017 (formato PDF, 783 kB).