Privacynews

Tecnologie e Comunicazioni **23/11/2017** Num. 5

Le linee guida del WP29 sul "Data Breach"

Il prossimo 28 novembre scadono i termini per l'invio di osservazioni alle "Guidelines on Personal data breach notification under Regulation 2016/679" adottate il 3 ottobre 2017 dal WP29. Vale la pena dare uno sguardo al testo proposto, in attesa che venga rilasciato il testo definitivo.

Le linee guida proposte forniscono una definizione abbastanza ampia di "violazione dei dati personali", che comprende non solo una violazione della riservatezza (ad es. divulgazione o accesso non autorizzati o accidentali a dati personali) e/o dell'integrità dei dati personali (ad es. alterazione non autorizzata o accidentale dei dati personali), ma anche una **perdita permanente** della disponibilità di dati personali.

Rientrano in quest'ultimo caso, ad esempio, la cancellazione di dati avvenuta accidentalmente o effettuata da persone non autorizzate, la perdita della chiave di decrittazione di un file criptato (e che pertanto non è più utilizzabile) o la impossibilità di eseguire un restore dei dati perché il back up non funziona.

Come è noto, il titolare del trattamento deve notificare una violazione entro 72 ore dal momento in cui ne sia venuto a conoscenza; le linee guida chiariscono che "essere venuti a conoscenza" significa, ad esempio che sono stati fatti accertamenti su eventuali segnalazioni, anche preliminari, da parte degli strumenti a presidio della protezione dati e che tali accertamenti abbiano indicato la possibilità di una violazione e si è quindi raggiunto un "**ragionevole grado di certezza**" dell'avvenuta violazione, anche se magari non tutte le conseguenze sono state analizzate. Può addirittura avvenire che il titolare sia contattato da un hacker per un riscatto per un malware iniettato nel sistema: questo è ovviamente il momento dal quale decorrono le 72 ore. Nel caso che un Titolare

Notizie dal Garante

Convegno Consumers' Forum
"Dalla sharing alla social, alla data economy. Big data, fake news, privacy e pubblicità"
27 novembre 2017 - 9,30/13,30
Sala Danilo Longhi presso Unioncamere Piazza Sallustio 21 - Roma.

Attacco hacker a Uber:
Dichiarazione di Antonello Soro, Presidente dell'Autorità Garante per la privacy
"Non possiamo che esprimere forte preoccupazione per la violazione subita da Uber**, tardivamente denunciata** dalla società americana. Abbiamo aperto un'istruttoria e stiamo raccogliendo tutti gli elementi utili per valutare la portata del data breach e le azioni da intraprendere a tutela degli eventuali cittadini italiani coinvolti. Quello che certo colpisce, in una multinazionale digitale come Uber, è **l'evidente insufficienza di adeguate misure di sicurezza** a protezione dei dati e quello che sconcerta è la scarsa trasparenza nei confronti degli utenti sulla quale indagheremo".
Roma, 22 novembre 2017

si avvalga di un Responsabile del trattamento, è probabile che le indagini vengano svolte dal Responsabile stesso, il quale può effettuare la notifica della violazione all'Autorità di controllo per conto del Titolare, sul quale comunque grava l'obbligo legale della notificazione.

Pertanto, nei rapporti contrattuali tra Titolare e Responsabile, è opportuno che venga inserita **una clausola in forza della quale il Responsabile comunica al Titolare senza alcun ritardo** l'informazione della possibile avvenuta violazione di dati personali, anche se le indagini sono ancora in corso.

Le linee guida chiariscono anche che non è sufficiente che i titolari o i responsabili abbiano adottate appropriate misure di sicurezza per essere esentati dalla notificazione, perché è sempre necessario guardare alle **conseguenze della violazione per gli interessati**.

I Garanti europei incoraggiano la notifica provvisoria, quando non tutte le informazioni sono disponibili all'inizio (cioè entro 72 ore), con la possibilità di modificare o migliorare una notifica a valle man mano che maggiori informazioni vengono alla luce in seguito.

Il GDPR dispone che, qualora vi sia un rischio elevato per il diritto e la libertà delle persone a seguito di una violazione, è necessario anche informare gli interessati direttamente, usando- come chiariscono le linee guida - metodi di comunicazione trasparenti (ad es. messaggistica diretta come email, sms, anche in lingue diverse) o una comunicazione pubblica, in caso sia uno sforzo sproporzionato raggiungere tutti gli interessati direttamente o nel caso, ad esempio, che vengano persi gli indirizzi e-mail. Le linee guida chiedono al Titolare anche di fornire indicazioni agli interessati su come proteggersi dalle possibili conseguenze negative della violazione (come ad esempio la reimpostazione delle password).

Molto rilevante è il concetto di responsabilità. Il WP29 fornisce indicazioni sulle principali attività da porre in essere, in particolare: a) valutare i rischi, adottare misure efficaci per contenere e affrontare la violazione e adottare adeguate misure di sicurezza; b) introdurre un registro interno di tutte le violazioni avvenute, indipendentemente dal fatto che siano soggette a notifica o meno, a registrare i dettagli relativi alla violazione, comprese le cause, gli effetti e le conseguenze, insieme alle azioni correttive adottate dal responsabile del trattamento; c) conservare la documentazione di tutte le violazioni, tra cui, ad esempio, se una violazione non viene notificata, una giustificazione per tale decisione.

Diventa quindi fondamentale per i Titolari preparare ed emanare un procedura interna per la gestione delle violazione di dati personali, che definisca il processo da seguire una volta rilevata una violazione, incluso come contenere, gestire e recuperare l'incidente assieme alla documentazione relativa al fine di dimostrare la conformità con GDPR, senza tener conto del fatto che non rispettare l'obbligo di notifica può portare a sanzioni severe.