News - 28/06/2019

# Le comunicazioni di data breach in base alle previsioni del Regolamento (UE) 2016/679

## Cosa fare in caso di violazione dei dati personali?

L'articolo 4 punto 12 del Regolamento Europeo n. 679/2016 definisce con il termine “data breach” una violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati.
Una violazione può comportare significativi effetti negativi sulle persone fisiche, quali ad esempio la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l’usurpazione d’identità, il pregiudizio alla reputazione, nonché qualsiasi altro danno economico o sociale. Al fine di prevenire i suindicati rischi, il Regolamento Europeo 2016/679 (GDPR) ha introdotto agli articoli 33 e 34 l’obbligo per il titolare del trattamento di dare comunicazione dell’avvenuta violazione di sicurezza sia all’autorità sia agli interessati.
In particolare, per quanto attiene alla comunicazione da effettuare nei confronti dell’autorità di controllo, l’articolo 33 del Regolamento Europeo impone al titolare del trattamento di notificare l’avvenuta violazione al Garante per la protezione dei dati personali, senza indebiti ritardi e ove possibile entro 72 ore dalla scoperta, qualora la predetta violazione comporti un rischio per i diritti e la libertà delle persone fisiche. Nell’ipotesi in cui la notifica non avvenga nelle 72 ore, il titolare del trattamento dovrà indicare i motivi del ritardo.
Ai sensi dell’ articolo 33 paragrafo 3 del Regolamento, la notifica deve contenere:

- la descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

Inoltre, se la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, l’articolo 34 del Regolamento dispone che la comunicazione venga effettuata anche nei confronti degli interessati. In tal caso il titolare del trattamento è obbligato a comunicare all’interessato, nel più breve tempo possibile e in modo chiaro e specifico la natura dell’avvenuta violazione e le informazione di cui al paragrafo 3 dell’articolo 33 del Regolamento. Viceversa, l’articolo 34 esclude il suddetto obbligo se il titolare del trattamento ha messo in atto adeguate misure tecniche ed organizzative di protezione e se ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati. Il medesimo articolo esclude l’obbligo di comunicazione individuale all’interessato qualora richiederebbe sforzi sproporzionati, ammettendo in tale ipotesi una comunicazione pubblica o una misura simile, tramite la quale gli interessati possano essere ugualmente informati della violazione con analoga efficacia. Sul punto è opportuno ricordare che Linee Guida dei Garanti europei n. WP250 del 3 ottobre 2017, aggiornate il 6 febbraio 2018, prevedono la possibilità per il titolare trattamento di contattare e consultare il Garante della privacy sia per chiedere consiglio sull’opportunità di informare gli interessati della violazione sia sui messaggi appropriati da inviare e sul modo più opportuno per contattare gli stessi. In particolare, il tritolare del trattamento nel comunicare una violazione agli interessati deve utilizzare messaggi dedicati che non siano inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi standard. Esempi di metodi trasparenti di comunicazione sono: la messaggistica diretta (ad esempio messaggi di posta elettronica, SMS, messaggio diretto), banner o notifiche su siti web di primo piano, comunicazioni postali e pubblicità di rilievo sulla stampa. Una semplice comunicazione all’interno di un comunicato stampa o di un blog aziendale non costituirebbe un mezzo efficace per comunicare una violazione all’interessato. Pertanto le Linee Guida raccomandano al titolare del trattamento di servirsi di mezzi che massimizzino la possibilità di comunicare correttamente le informazioni a tutte le persone interessate, comportando ciò l’utilizzo da parte dello stesso di diversi metodi di comunicazione, anziché un singolo canale di contatto.