Procedura per la gestione del data breach e rendicontazione incidenti/violazioni dei dati

Gli artt. 33 e 34 del Regolamento europeo 679/2016 disciplinano le modalità di gestione del data breach da parte del Titolare del trattamento e le situazioni in cui risulta necessaria la notifica al Garante di avvenuta violazione.

Come definito dal considerando 85, la violazione dei dati è tale se provoca danni fisici, materiali o immateriali alle persone fisiche (es. perdita di controllo dei dati personali che li riguardano o limitazione dei propri diritti, discriminazione, furto o usurpazione di identità, perdita finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata).

1 - Quando effettuare la notifica al Garante:

Nel caso in cui la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (come descritte dal considerando 85), il Titolare del trattamento deve notificare l'avvenuta violazione all'autorità di controllo italiana (Garante per la privacy) entro le 72 ore dal momento in cui ne è venuto a conoscenza o comunque senza ingiustificato ritardo. Qualora la notifica all'autorità di controllo non venga effettuata entro le 72 ore, il Titolare del trattamento dovrà motivarne il ritardo.

La notifica deve almeno:

a. descrivere la 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;
b. comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c. descrivere le probabili conseguenze della violazione dei dati personali;
d. descrivere 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 anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

La comunicazione al Garante va effettuata all'indirizzo protocollo@pec.gpdp.it è in fase di definizione da parte dell'autorità di controllo l'attivazione della procedura telematica di comunicazione del data breach.

2 - Quando effettuare la notifica all'interessato:

Salvo i casi in cui risulti improbabile, il Titolare del trattamento deve notificare agli interessati la violazione dei dati subìta solo nei casi in cui le conseguenze del data breach siano tali da comportare un rischio elevato per i diritti e le libertà delle persone fisiche. La notifica può anche non essere effettuata se il Titolare del trattamento ha provveduto (in via preventiva o successiva) ad adottare le misure atte ad evitare effetti negativi sui soggetti interessati.

3 - Quando non effettuare la notifica:

Se la violazione dei dati personali non provoca danno di cui al considerando 85, il Titolare del trattamento non deve effettuare alcuna comunicazione né al Garante né all'interessato.

4 - Tenuta del incidenti/violazioni dei dati:

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo. Nello schema sotto riportato è indicato una tabella di rendicontazione delle violazioni subìte che il Titolare del trattamento dovrà mettere a disposizione dell'autorità di controllo, in caso di necessità. Con il registro dovranno, inoltre, essere conservati i documenti di comunicazione inviati al Garante.

Denominazione violazione	Data e ora violazione	Banca dati oggetto della violazione	Descrizione della violazione	Effettuazione della comunicazione all'autorità di controllo	Persona fisica addetta alla comunicazione
