AUTOMOBILE CLUB MILANO

DATA BREACH: PIANO DI SICUREZZA e PROCEDURA OPERATIVA

Regolamento UE 2016/679 in materia di protezione dei dati personali

Il presente documento riepiloga le azioni da intraprendere in caso di violazione dei dati personali.

Una violazione dei dati personali (cosiddetto «*data breach*») consiste in una «*violazione di 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*» (Art. 4, definizione 12).

La violazione può essere determinata da accesso abusivo ai sistemi informatici, ovvero da sottrazione o perdita di dati e supporti di memorizzazione.

Al verificarsi di un *data breach* il Titolare (nella persona, nel caso, del Direttore dell'Ente, col supporto dei responsabili nominati, dell'amministratore di sistema e dei tecnici informatici, nonché del DPO) deve valutare se vi sia un rischio elevato per i diritti e le libertà delle persone fisiche (art. 33). Se valuta che vi sia tale rischio, occorre notificare alle Autorità Garanti, senza ingiustificato ritardo (e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza) le violazioni dei dati e comunicarle agli interessati senza ingiustificato ritardo.

La notifica all'Autorità deve, fra l'altro, descrivere:

- la natura della violazione dei dati personali;
- 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;
- 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 anche, se del caso, per attenuarne i possibili effetti negativi.

Se invece valuta che non vi sia rischio elevato per i diritti e le libertà delle persone fisiche, Il Titolare del trattamento deve comunque documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, al fine di consentire all'autorità di controllo di verificare il rispetto di quanto previsto nell'art. 33. Per i dati trattati dai soggetti terzi, il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

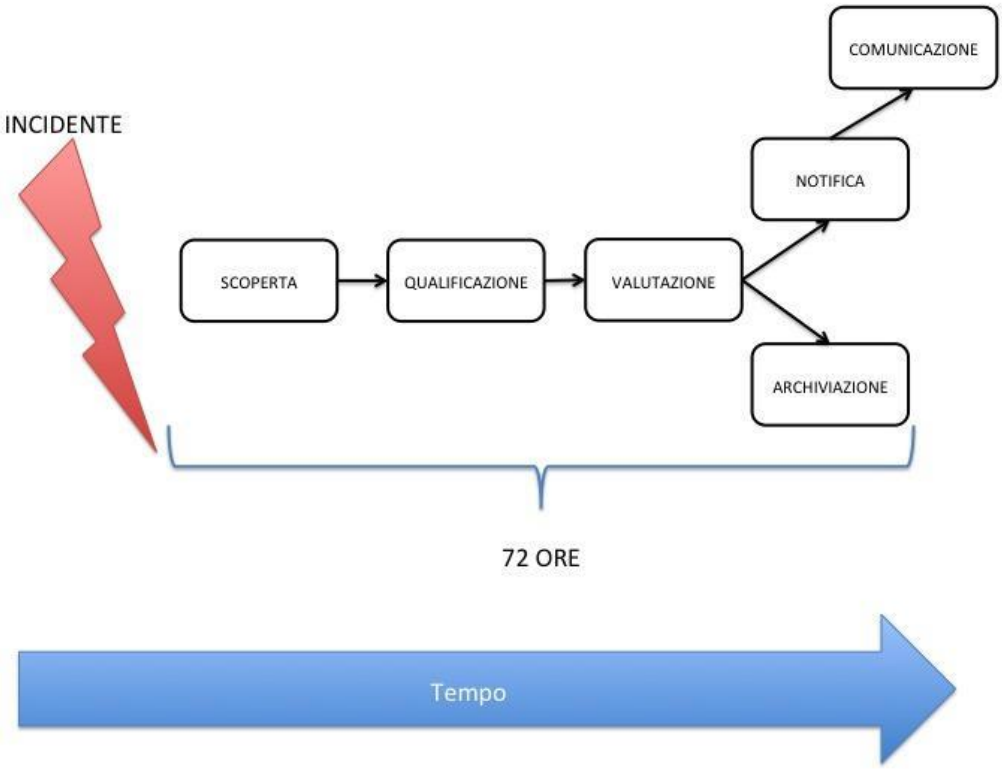
Il titolare è tenuto a documentare il modo in cui viene a conoscenza della violazione. Ritardi nell'individuazione del *data breach*, dovute a carenza di misure tecniche e organizzative, o ad omessi controlli interni, costituiscono elementi che il Garante può vagliare in sede di provvedimenti o di eventuali misure sanzionatorie.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento è tenuto a comunicare la violazione all'interessato senza ingiustificato ritardo (art. 34). Tale comunicazione è volta a ridurre il danno che può derivare all'interessato in conseguenza della violazione (consentendogli di adottare contromisure idonee a contenere gli effetti dannosi della violazione).

La comunicazione all'interessato non è richiesta se erano state applicate ai dati oggetto della violazione adeguate misure di sicurezza destinate a rendere i dati personali incomprensibili (quali la cifratura) oppure se sono successivamente adottate misure atte a scongiurare un rischio elevato. La valutazione sulla necessità della comunicazione è in capo al titolare, anche se l'Autorità può obbligarlo ad effettuarla nel caso in cui non l'avesse ritenuta necessaria.

Procedura in caso di *data breach*

I processi che descrivono la successione temporale di procedure e azioni in caso di *data breach* sono descritti nella seguente immagine, e devono svilupparsi nell'arco temporale massimo di 72 ore:



Nell'eventualità in cui si constati o si sospetti un evento di *data breach* (***scoperta***), il dipendente deve informare tempestivamente il Direttore dell'Ente, indicando gli elementi utili ad avviare gli approfondimenti del caso (***qualificazione***): data dell'evento, ammontare e tipologia di dati coinvolti, categoria di interessati, modalità attraverso cui è avvenuto l'incidente e come è stato rilevato, ecc...

Entro 12 ore dev'essere informato l'RPD ed il gruppo di supporto al RPD, nonché i tecnici informatici per la gestione dell'incidente e la continuità operativa.

Il Titolare, unitamente ai soggetti coinvolti nella gestione del *data breach*, deve:

- raccogliere le informazioni necessarie al fine di chiarire la veridicità, la portata e la reale sussistenza dell'evento segnalato;
- individuare eventuali soggetti autorizzati che devono essere coinvolti per la raccolta di ulteriori informazioni;
- valutare prioritariamente eventuali azioni per contenere gli effetti dell'evento, comprese precise istruzioni da dare ai soggetti autorizzati coinvolti;

- definire se l'evento segnalato integri una violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche.

In particolare, ai fini della eventuale segnalazione all'Autorità garante, il Titolare deve valutare le conseguenze della violazione dei dati personali per gli interessati coinvolti e la gravità della violazione, ovvero:

a) se sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche; b) se sia necessario effettuare una comunicazione del *data breach* agli interessati coinvolti;

c) quali misure di mitigazione adottare per interrompere gli effetti del *data breach* o contenerne gli effetti.

Nel caso a) non è necessario procedere alla notifica all'Autorità garante o nei confronti degli interessati. L'incidente viene archiviato ma viene in tutti i casi inserito un record nel registro interno delle violazioni (Registro *Data Breach*). Gli eventi di sicurezza che non comportano un trattamento di dati personali o i meri bug non devono essere riportati nel Registro.

L'analisi dei rischi è effettuata seguendo i criteri di cui alle "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 WP250rev.01 - Gruppo di lavoro Articolo 29 per la protezione dei dati".

Nel caso b), entro le successive 24 ore il Titolare ***notifica*** all'Autorità Garante l'incidente. La notifica deve perlomeno:

1. 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;
2. comunicare il nome e i dati di contatto del RPD;
3. descrivere le probabili conseguenze della violazione dei dati personali;
4. 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;
5. deve essere utilizzato il modello predisposto dal Garante per la protezione dei dati personali pubblicato al seguente indirizzo: https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni .

In base alla valutazione del Titolare, sentito il RPD, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento ***comunica*** la violazione all'interessato senza ingiustificato ritardo. La comunicazione avviene ad opera dell'ufficio individuato in relazione all'interessato/i coinvolto/i e descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno i punti 2), 3) e 4) dell'elenco precedente.

Nell'eventualità in cui detta comunicazione richiederebbe sforzi sproporzionati, la violazione viene resa pubblica attraverso canali generici quali ad esempio un avviso sul portale web ovvero utilizzando i Social Media.

In base alla valutazione del Titolare e dell'RPD, non si procede con la comunicazione all'interessato se:

1. il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
2. il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

3. la comunicazione richiederebbe sforzi sproporzionati e si è adottato il metodo della comunicazione pubblica come precedentemente indicato.

In caso di eventi particolarmente gravi o complessi, la qualificazione e successiva analisi dell'evento stesso di *data breach* può richiedere un processo di approfondimento con tempistiche incompatibili rispetto ai termini di legge (72 ore dalla scoperta, Regolamento UE 2016/679, art. 33). In tal caso, il Titolare, se non è in grado di raccogliere tutte le informazioni richieste entro il termine, effettua comunque la prima notifica entro le 72 ore e effettua successivamente ulteriori notifiche integrative.

Milano, 20 marzo 2023

Il Direttore
Dott. Paolo Roggero