UNIVERSITÀ DI TRENTO

Procedura di Gestione delle Violazioni di Dati Personali (*Data Breach*) UniTrento vers. 3.0

– Marzo 2022 –

Sommario

1. Definizioni

Di seguito riportiamo le principali definizioni della terminologia utilizzata nel presente documento.

1.1. Violazione di dati personali *(data breach)*

La violazione di sicurezza che comporta accidentalmente o in modo illecito la Distruzione, Perdita, Modifica, Divulgazione o accesso non autorizzati ai dati personali trasmessi, conservati o comunque trattati.

1.2. Distruzione *(destruction)*

Non esistono più i dati ovvero i dati non esistono più in una forma che possa essere utilizzata dal Titolare.

1.3. Modifica *(alteration, damage)*

I dati risultano alterati, corrotti o incompleti

1.4. Perdita *(loss)*

I dati esistono ancora, ma il Titolare non ne ha più il controllo o l'accesso ovvero il Titolare non ha più i dati.

1.5. Divulgazione *(unauthorized or unlawful processing)*

I dati sono oggetto di divulgazione o accesso da parte di destinatari non autorizzati, oppure qualsiasi forma di trattamento effettuato in violazione del GDPR.

1.6. RPD e RTD

Le figure del Responsabile per la Protezione dei dati e del Responsabile della Transizione al Digitale come individuati nel contesto organizzativo dell'Ateneo.

1.7. CERT@unitn

Il presidio organizzativo di Ateneo per la gestione degli incidenti di sicurezza ICT.

1.8. Preposto al trattamento

Il Responsabile delle strutture di I° livello di Ateneo delegato dal Titolare alla gestione presso la propria struttura degli adempimenti imposti dal GDPR.

2. Caratteristiche delle violazioni di dati personali

La violazione di dati personali (*data breach*) è un incidente di sicurezza. Solo nel caso siano coinvolti dati personali si applicano le prescrizioni dettate dal GDPR.

Nel caso in cui non siano coinvolti dati personali l'incidente di sicurezza deve essere comunque segnalato al CERT@unitn anche per una eventuale segnalazione al CERT-PA.

Si possono distinguere tre categorie di violazioni di dati:

- **Violazione della Riservatezza** *(Confidentiality Breach):*
  Quando si ha una divulgazione di dati o un accesso agli stessi non autorizzato o accidentale;
- **Violazione dell'Integrità** *(Integrity Breach):*
  Quando il dato è alterato in modo accidentale o non autorizzato;
- **Violazione della Disponibilità** *(Availability Breach):*
  Quando in modo accidentale o per dolo il Titolare non accede ai dati o i dati sono stati distrutti.

Una violazione di dati personali può comprendere una o tutte e tre le categorie o anche loro combinazioni.

Ci sarà sempre una violazione della **Disponibilità** del dato nel caso di perdita o distruzione permanente dei dati. L'indisponibilità dei dati è quindi da considerare una violazione quando potrebbe avere un impatto significativo sui diritti e le libertà delle persone fisiche. Non si tratta invece di una violazione quando l'indisponibilità è dovuta a interruzioni programmate per la manutenzione.

3. Procedura di comunicazione della violazione di dati personali

Si individua di seguito i soggetti coinvolti e il flusso delle principali attività previste per la rilevazione e gestione di un incidente di sicurezza che può comportare una violazione di dati personali.

Il coordinamento delle attività di gestione di una violazione di dati personali, con particolare riferimento agli obblighi di comunicazione e notifica imposti dal GDPR, è assicurato, su delega del Titolare del trattamento, dal RPD o, in sua assenza dal RTD, con il supporto del CERT@unitn per gli aspetti tecnici e dell'Ufficio Legale per gli aspetti giuridici nonché dal Responsabile della struttura interessata dalla violazione.

3.1. Rilevazione e segnalazione di una potenziale violazione

Chi	Tutto il personale, Collaboratori, Fornitori, Responsabili, Preposti, Titolare, CERT@unitn, utenti esterni, GARR-CERT, RPD
A chi	Al Responsabile della struttura/Preposto al trattamento (Dirigente, Direttore di Dipartimento/Centro) o suo delegato anche tramite il referente privacy della struttura stessa (in mancanza di tali figure direttamente al CERT@unitn)
Quando	Appena se ne viene a conoscenza
Come	Utilizzando le vie più brevi (telefonicamente, di persona, via e-mail)

3.2. Raccolta informazioni sulla potenziale violazione

Chi	Il Responsabile della struttura/Preposto al trattamento o suo delegato anche tramite il referente privacy insieme ai soggetti coinvolti nell'incidente. A seguito di una segnalazione, il responsabile/preposto deve coordinare la raccolta delle informazioni nel più breve tempo possibile anche con il supporto del RPD e del CERT@unitn
Quando	Appena ricevuta la segnalazione
Come	Utilizzando il modulo fornito (Allegato A) e raccogliendo tutte le informazioni dai soggetti coinvolti nella segnalazione

3.3. Comunicazione della potenziale violazione

Chi	Il Responsabile della struttura/Preposto al trattamento o suo delegato anche tramite il referente privacy
A chi	RPD, CERT@unitn, Titolare
Quando	Appena ottenute le informazioni sulla potenziale violazione

Come	Inviando il modulo fornito debitamente compilato o, qualora ciò non sia possibile, utilizzando le vie più brevi

3.4. Valutazione d'impatto della violazione

Chi	Titolare, RPD, soggetti coinvolti
Quando	Appena ricevuta la comunicazione
Come	Valutando la gravità dell'impatto della violazione sulla base delle informazioni disponibili e i fattori indicati in 7.

3.5. Individuazione delle azioni correttive

Chi	RPD, CERT@unitn, soggetti coinvolti
Quando	Appena completata la valutazione d'impatto

3.6. Comunicazione delle valutazioni effettuate e delle azioni da intraprendere

Chi	RPD, Responsabile della struttura/Preposto al trattamento o suo delegato anche tramite il referente privacy
A chi	Titolare
Quando	Appena completata la valutazione d'impatto e l'eventuale individuazione delle azioni correttive

3.7. Notifica della violazione (se è necessaria)

Chi	Titolare
A chi	Garante
Quando	Entro 72 ore dalla rilevazione della violazione
Come	Compilando il modulo fornito per la notifica al Garante

3.8. Comunicazione agli interessati coinvolti (se è necessaria)

Chi	Titolare
A chi	Alle persone fisiche i cui dati sono stati violati

Quando	Nei termini indicati nella valutazione d'impatto
Come	Contattando direttamente gli interessati oppure rendendo nota la violazione e le possibili conseguenze mediante pubblicazione accessibile alle categorie di interessati

3.9. Disposizioni per l'attuazione delle misure correttive (se individuate)

Chi	Responsabili delle strutture coinvolte
A chi	Soggetti incaricati di svolgere le attività
Quando	Nei termini indicati nella valutazione d'impatto
Come	Devono essere indicate in dettaglio le operazioni da svolgere, il soggetto incaricato e i tempi di attuazione, prevedendo eventuali attività di verifica dell'efficacia delle misure correttive

3.10. Recepimento della risposta del Garante alla notifica (se effettuata)

Chi	Titolare, RPD, Responsabili delle strutture coinvolte, CERT@unitn
Come	Attuare le eventuali misure correttive indicate dal Garante

4. Attività relative alla registrazione della violazione

Di seguito si individuano i soggetti coinvolti e il flusso delle principali attività riconducibili all'obbligo di registrazione delle violazioni in un registro.

4.1. Registrazione della violazione

Chi	RPD
Quando	Appena ricevuta la comunicazione della violazione
Come	Compilando l'apposito registro delle violazioni

4.2. Registrazione della risposta del Garante (se effettuata la notifica)

Chi	RPD
Quando	Appena ricevuta la risposta dal Garante
Come	Annotando sul registro la risposta del Garante e le eventuali prescrizioni in essa contenute

4.3. Registrazione della prosecuzione delle indagini o chiusura dell'incidente

Chi	RPD
Quando	Appena ricevuta la comunicazione di prosecuzione delle indagini o di chiusura dell'incidente
Come	Annotando sul registro le istruzioni per le ulteriori indagini o la chiusura dell'incidente se non necessita di ulteriori indagini o azioni

5. Attività inerenti la prosecuzione delle indagini

Di seguito si individuano i soggetti coinvolti e il flusso delle principali attività riconducibili alla necessità di ulteriori indagini.

5.1. Prosecuzione delle indagini (se necessario)

Chi	RPD, Responsabile della struttura/Preposto al trattamento o suo delegato anche tramite il referente privacy insieme ai soggetti coinvolti nella violazione, CERT@unitn
Quando	A seguito di indicazione da parte del Garante o del Titolare, se previsto nella prima valutazione d'impatto della violazione o nel caso le informazioni raccolte risultino incomplete o mancanti
Come	Raccogliendo e/o completando le informazioni mancanti o approfondendo le informazioni già note per rilevare eventuali potenziali impatti della violazione non riscontrati nella prima fase di indagine

5.2. Comunicazione dei risultati della prosecuzione delle indagini

Chi	RPD, Responsabile della struttura/Preposto al trattamento o suo delegato anche tramite il referente privacy
A chi	Titolare, RPD
Quando	Appena terminate le ulteriori indagini
Come	Inviando il modulo fornito per la segnalazione o una relazione sulle ulteriori informazioni raccolte

5.3. Esecuzione di una nuova valutazione d'impatto

Chi	Titolare, RPD, soggetti coinvolti nella violazione
Quando	Al momento in cui si ritiene di aver raccolto tutte le ulteriori informazioni sulla violazione necessarie e sufficienti per eseguire una nuova valutazione
Come	Valutando la gravità dell'impatto della violazione sulla base delle ulteriori informazioni disponibili e i fattori indicati in 7 e individuando le eventuali azioni correttive

5.4. Aggiornamento della notifica al Garante (se necessario)

Chi	Titolare
Quando	Appena sono disponibili le informazioni ulteriori o secondo le indicazioni comunicate dal Garante
Come	Compilando il modulo fornito per la notifica al Garante

5.5. Comunicazioni agli interessati (se necessario)

Chi	Titolare
A chi	Alle persone fisiche i cui dati sono stati violati
Quando	Nei termini indicati nella valutazione d'impatto
Come	Contattando direttamente gli interessati oppure rendendo nota la violazione e le possibili conseguenze mediante pubblicazione accessibile alle categorie di interessati

6. Informazioni da raccogliere relative alla violazione

Il Responsabile della struttura/Preposto al trattamento o suo delegato anche tramite il referente privacy insieme ai soggetti coinvolti nell'incidente coordina la raccolta delle informazioni nel più breve tempo possibile anche con il supporto del RPD e del CERT@unitn.

Se al momento della rilevazione dell'incidente di sicurezza non è disponibile una descrizione particolareggiata dell'evento, è comunque essenziale procedere immediatamente alla comunicazione dell'incidente per una prima valutazione d'impatto, anche con informazioni incomplete. Laddove necessario alla prima valutazione possono seguirne altre, in base alle informazioni che vengono acquisite nella prosecuzione dell'indagine.

Le informazioni che sono necessarie per effettuare la valutazione d'impatto dell'incidente e conseguentemente l'eventuale notifica della violazione al Garante e la comunicazione alle persone fisiche interessate sono da raccogliere utilizzando l'apposito modulo pubblicato nella sezione privacy del portale di Ateneo.

L'eventuale notifica al Garante viene effettuata dal Titolare utilizzando il modulo di cui all'allegato A.

.

7. Valutazione della gravità della violazione

La gravità di una violazione di dati personali è definita come la stima dell'entità del potenziale impatto sulle persone fisiche derivante dalla violazione medesima.

La tabella seguente presenta i principali fattori definiti nelle linee guida WP250 del Gruppo di Lavoro Art. 29[1] che devono essere considerati nella valutazione di impatto della gravità di una violazione sulla base delle informazioni raccolte.

Tale valutazione di impatto permette di stabilire la necessità di notifica della violazione al Garante, in particolare se probabile un rischio per la libertà e diritti delle persone fisiche e la comunicazione anche agli interessati, nel caso in cui tale rischio sia elevato.

Fattori considerati nella valutazione del rischio per i diritti e le libertà delle persone fisiche interessate dalla violazione

Aspetti generali	Valutazione della gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche e della probabilità che tale impatto si verifichi
Tipo di violazione	Come specificato in paragrafo 1. Definizioni (Distruzione, Modifica, Perdita, Divulgazione)
Natura, carattere sensibile e volume dei dati personali	Categorie particolari di dati o combinazione di dati personali, grandi quantità di dati personali relative a molte persone coinvolti nella violazione
Facilità di identificazione delle persone fisiche	Facilità di identificazione, diretta o indiretta tramite abbinamento con altre informazioni, di specifiche persone fisiche sulla base dei dati personali compromessi dalla violazione
Gravità delle conseguenze per le persone fisiche	Danno potenziale alle persone fisiche che potrebbe derivare dalla violazione comprese le categorie degli interessati e dei dati personali coinvolti e la permanenza a lungo termine delle conseguenze del danno (furto di identità, danni fisici, disagio psicologico, danni di immagine/reputazione)
Caratteristiche particolari del titolare	Nel contesto delle sue attività istituzionali l'Università è, in particolare, titolare dei dati personali trattati per le finalità di ricerca

[1] "Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250**"** adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017 - versione emendata e adottata il 6 febbraio 2018.

Caratteristiche particolari dell'interessato	La violazione coinvolge in particolare dati personali di minori o altre persone fisiche vulnerabili
Numero di persone fisiche interessate	Numero di persone fisiche coinvolte nella violazione

8. Modalità di notifica di una violazione di dati personali al Garante per la protezione dei dati personali

Si considerano parte integrante della presente procedura le indicazioni dell'Autorità Garante sulla notifica di violazione dei dati personali pubblicate alla pagina https://www.garanteprivacy.it/regolamentoue/databreach in relazione alle modalità di notifica, alla modulistica e alle informazioni da indicare.