UNIVERSITÀ DELLA VALLE D'AOSTA
UNIVERSITÉ DE LA VALLÉE D'AOSTE

2019

Procedura di Gestione delle Violazioni di Dati Personali (Data Breach)

UNIVERSITÀ DELLA VALLE D'AOSTA – UNIVERSITÉ DE LA VALLÉE D'AOSTE

VERSIONE 1.0 MAGGIO 2019

UNIVERSITÀ DELLA VALLE D'AOSTA
UNIVERSITÉ DE LA VALLÉE D'AOSTE

Sommario

UNIVERSITÀ DELLA VALLE D'AOSTA
UNIVERSITÉ DE LA VALLÉE D'AOSTE

DEFINIZIONI

Si intende per:

violazione dei dati personali (Data Breach): una 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;

distruzione dei dati: condizione in cui i dati non esistono più ovvero i dati non esistono più in una forma che possa essere utilizzata dal Titolare;

modifica dei dati: condizione in cui i dati risultano alterati, corrotti o incompleti;

perdita dei dati: condizione in cui i dati esistono ancora ma il Titolare non ne ha più il controllo o l'accesso ovvero il Titolare non ha più i dati;

divulgazione dei dati: condizione in cui i dati sono oggetto di divulgazione o accesso da parte di destinatari non autorizzati, oppure qualsiasi forma di trattamento effettuato in violazione del GDPR;

DPO: il Responsabile per la Protezione dei dati di Ateneo;

Titolare: il Titolare del trattamento.

COS'E UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)?

Una violazione di dati personali (Data Breach) è un incidente di sicurezza che comporti, 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 dal Titolare del trattamento.

L'incidente di sicurezza deve essere comunicato ai Sistemi Informatici di Ateneo.

Si possono distinguere tre categorie di violazioni di dati:

a) violazione della riservatezza: quando si ha una divulgazione di dati o un accesso agli stessi non autorizzato o accidentale;
b) violazione dell'integrità: quando il dato è alterato in modo accidentale o non autorizzato;
c) violazione della disponibilità: 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.

Una violazione della riservatezza o dell'integrità del dato è facilmente individuabile. Meno chiara è l'individuazione di una violazione della disponibilità del dato. 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.

A titolo esemplificativo e non esaustivo, le violazioni di dati personali possono includere:

1. divulgazione di dati personali a soggetti non autorizzati;
2. perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
3. perdita o furto di documenti cartacei;

4. infedeltà aziendale (ad esempio: Data Breach causato da una persona interna che, avendo autorizzazione ad accedere ai dati, ne produce una copia che viene distribuita in ambiente pubblico);
5. accesso abusivo (ad esempio: Data Breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
6. casi di pirateria informatica (usurpazione delle credenziali di accesso – fishing);
7. banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
8. virus o altri attacchi al sistema informatico o alla rete aziendale;
9. violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o armadi contenenti archivi con informazioni riservate);
10. smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
11. invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

A CHI SONO RIVOLTE QUESTE PROCEDURE?

Queste procedure sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento:

a) i lavoratori dipendenti, nonché coloro che a qualsiasi titolo, e quindi a prescindere dal tipo di rapporto contrattuale intercorrente, abbiano accesso ai dati personali trattati nel corso delle prestazioni richieste per conto del Titolare del trattamento;
b) qualsiasi soggetto (persona fisica o persona giuridica) diverso dal destinatario interno che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento, abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare;

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

A QUALI TIPI DI DATI SI RIFERISCE QUESTA PROCEDURA?

Questa procedura si riferisce a:

- dati personali trattati "da" e "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;
- dati personali conservati o trattati a mezzo di qualsiasi altro Sistema in uso in Ateneo.

Per «dato personale» si intende: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

UNIVERSITÀ DELLA VALLE D'AOSTA
UNIVERSITÉ DE LA VALLÉE D'AOSTE

GESTIONE DELLA VIOLAZIONE DI DATI PERSONALI

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.

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 dal DPO con il supporto dei Sistemi Informatici di Ateneo per gli aspetti tecnici e del Responsabile della struttura interessata dalla violazione.

Rilevazione e segnalazione di una potenziale violazione

Chi	chiunque ne venga a conoscenza (personale, collaboratori, fornitori, responsabili del trattamento, Titolare, utenti esterni, DPO, etc.)
A chi	al Responsabile della struttura (amministrativa, didattica o di ricerca) interessata dall'incidente di sicurezza e ai Sistemi Informatici di Ateneo
Quando	appena ne viene a conoscenza
Come	utilizzando le vie più brevi (telefonicamente, di persona, via e-mail)

Se al momento della rilevazione dell'incidente di sicurezza non è disponibile una descrizione particolareggiata dell'evento, è comunque essenziale procedere immediatamente alla comunicazione anche con informazioni incomplete.

Raccolta e analisi delle informazioni sulla potenziale violazione

Chi	il Responsabile della struttura interessata dall'incidente di sicurezza insieme ai soggetti coinvolti nell'incidente. A seguito di una segnalazione, il Responsabile della struttura deve coordinare la raccolta delle informazioni nel più breve tempo possibile, anche con il supporto del DPO e dei Sistemi Informatici di Ateneo
Quando	appena ricevuta la segnalazione
Come	utilizzando il modulo di cui all'Allegato A - Modulo di comunicazione Data Breach e raccogliendo tutte le informazioni dai soggetti coinvolti nella segnalazione

L'Allegato A, debitamente compilato, permette di condurre una valutazione iniziale al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto.

Una volta stabilito che un Data Breach è avvenuto il Titolare del trattamento (o suo delegato), insieme al DPO, deve stabilire:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (es. riparazione fisica di strumentazione, utilizzo dei file di back up per recuperare dati persi o danneggiati, isolamento/chiusura di un settore compromesso della rete, cambio dei codici di accesso, etc.);
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento e il DPO valuteranno la gravità della violazione utilizzando l'allegato B - Modulo di valutazione del Rischio connesso al Data Breach che dovrà essere esaminato unitamente all'Allegato A, tenendo, altresì, in debita considerazione i principi e le indicazioni di cui agli artt. 33 e 34 del GDPR.

Notifica della violazione all'Autorità Garante (se necessaria)

Chi	il Titolare
A chi	all'autorità Garante
Quando	senza ingiustificato ritardo e, ove possibile, entro 72 ore dalla rilevazione della violazione
Come	compilando il modulo messo a disposizione sul sito istituzionale dall'Autorità Garante

Una volta valutata la necessità di effettuare la notifica della violazione dei dati subita, l'Ateneo provvede senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.

Comunicazione agli interessati coinvolti (se necessaria)

Chi	il Titolare
A chi	alle persone fisiche i cui dati sono stati violati
Quando	senza ingiustificato ritardo
Come	contattando direttamente gli interessati oppure rendendo nota la violazione e le possibili conseguenze mediante pubblicazione accessibile alle categorie di interessati

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati agli interessati, l'Ateneo provvede senza ingiustificato ritardo.

La comunicazione deve contenere:

- il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate, o di cui si propone l'adozione da parte del Titolare del trattamento, per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, è possibile utilizzare una comunicazione pubblica.

Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente comunicato attraverso l'Allegato A, l'Ateneo è tenuto a documentarlo attraverso la compilazione dell'apposito Registro.

Il Registro dei Data Breach contiene almeno le seguenti informazioni:

- data e ora della violazione;
- natura della violazione;
- categorie di interessati coinvolte;
- categorie di dati personali coinvolte;
- effetti della violazione;
- contromisure adottate;
- se sia stata effettuata notifica all'Autorità Garante;
- se sia stata effettuata comunicazione agli interessati.

Il Registro dei Data Breach deve essere continuamente aggiornato e messo a disposizione del Garante, qualora l'Autorità chieda di accedervi.

UNIVERSITÀ DELLA VALLE D'AOSTA
UNIVERSITÉ DE LA VALLÉE D'AOSTE

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 (se è probabile un rischio per la libertà e diritti delle persone fisiche) e di 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	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 reputazionali)
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
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

[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.

UNIVERSITÀ DELLA VALLE D'AOSTA
UNIVERSITÉ DE LA VALLÉE D'AOSTE

Allegato A – Modulo di comunicazione Data Breach

Il presente modulo deve essere compilato dal Responsabile della struttura interessata dall'incidente di sicurezza insieme ai soggetti coinvolti nell'incidente, con il supporto del DPO e dei Sistemi Informatici di Ateneo, in caso di incidente di sicurezza che possa comportare una violazione di dati personali ai fini di una valutazione e gestione dell'incidente stesso e, in caso di violazione accertata, di notifica al Garante e di comunicazione agli interessati.

Le informazioni relative all'incidente devono essere raccolte prima possibile e il modulo compilato in ogni sua parte deve essere inviato al più presto all'indirizzo rpd@univda.it e u-sistemi@univda.it o trasmesso tramite il canale più breve disponibile al Titolare, al DPO o ai Sistemi Informatici di Ateneo.

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.

Informazioni di contatto

Dati identificativi del segnalante (nome e cognome): _____

Struttura di riferimento: _____

Telefono: _____ E-mail: _____

Informazioni sull'incidente di sicurezza

Data scoperta violazione	
Luogo dell'incidente	
Data e ora dell'incidente	
Descrizione sintetica dell'incidente	
Tipo di violazione	□ Lettura (presumibilmente è stato effettuato un accesso ai dati ma i dati non sono stati copiati) □ Copia (i dati sono ancora presenti sui sistemi del Titolare ma copiati dall'autore della violazione) □ Alterazione (i dati sono presenti sui sistemi del Titolare ma sono stati alterati) □ Cancellazione (i dati non sono più sui sistemi del Titolare e non sono neppure in possesso dell'autore della violazione) □ Furto (i dati non sono più sui sistemi del Titolare ma sono presumibilmente in possesso dell'autore della violazione) □ Indisponibilità (i dati sono presenti sui sistemi del Titolare ma non sono disponibili per un certo periodo di tempo) □ Altro: _____
Dispositivo oggetto della violazione	□ Computer □ Server

	□ Storage □ Rete □ Dispositivo mobile □ File o parte di un file □ Strumento di backup □ Documento cartaceo □ Altro: _____
Denominazione della/e banca/che dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati	
Categorie di soggetti coinvolti	□ Personale docente e ricercatore □ Personale tecnico amministrativo □ Studenti □ Minori □ Disabili □ Altri Utenti: _____
Categorie di dati personali oggetto della violazione	□ Dati anagrafici/codice fiscale □ Dati di contatto □ Dati di accesso e di identificazione (es. username, password, altro) □ Dati relativi a minori □ Dati relativi ad altri soggetti vulnerabili □ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati □ Dati economico finanziari (es. numero carta di credito, IBAN, etc.) □ Dati genetici □ Dati relativi alla salute □ Dati giudiziari □ Dati biometrici
Breve descrizione di eventuali azioni poste in essere al momento della scoperta della violazione	

UNIVERSITÀ DELLA VALLE D'AOSTA
UNIVERSITÉ DE LA VALLÉE D'AOSTE

Allegato B - Modulo di valutazione del rischio connesso al Data Breach

Dispositivi oggetto del Data Breach	□ Computer □ Server □ Storage □ Rete □ Dispositivo mobile □ File o parte di un file □ Strumento di backup □ Documento cartaceo □ Altro: _____
Modalità di esposizione al rischio (tipo di violazione)	□ Lettura (presumibilmente è stato effettuato un accesso ai dati ma i dati non sono stati copiati) □ Copia (i dati sono ancora presenti sui sistemi del Titolare ma copiati dall'autore della violazione) □ Alterazione (i dati sono presenti sui sistemi del Titolare ma sono stati alterati) □ Cancellazione (i dati non sono più sui sistemi del Titolare e non sono neppure in possesso dell'autore della violazione) □ Furto (i dati non sono più sui sistemi del Titolare ma sono presumibilmente in possesso dell'autore della violazione) □ Indisponibilità (i dati sono presenti sui sistemi del Titolare ma non sono disponibili per un certo periodo di tempo) □ Altro: _____
Breve descrizione dei sistemi di elaborazione o di memorizzazione dati coinvolti, con indicazione della loro ubicazione	*Descrizione*
Numero di persone colpite dalla violazione dei dati personali trattati nell'ambito della banca dati violata	*Descrizione*
Natura dei dati coinvolti (compilare le sezioni sottostanti):	*Descrizione*
a. dati personali generici	*Descrizione*
b. dati particolari, come identificati dal Regolamento (UE) 2016/679, relativi ad una persona viva ed individuabile: □ origine razziale o etnica □ opinioni politiche, convinzioni religiose e filosofiche □ appartenenza sindacale □ dati genetici □ dati biometrici □ dati giudiziari □ dati relativi alla salute o all'orientamento sessuale di una persona	*Descrizione*
c. informazioni che possono essere utilizzate per commettere furti d'identità (es. dati di accesso	*Descrizione*

e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito)	
d. informazioni personali relative a soggetti fragili (es. anziani, disabili, minori)	*Descrizione*
e. profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone	*Descrizione*
Altro:	*Descrizione*
La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo	Si/NO *Descrizione*
Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali che li riguardano	Si/NO *Descrizione*
Misure tecniche e organizzative adottate precedentemente alla violazione (es. Pseudonimizzazione, cifratura dei dati personali, etc.)	*Descrizione*
Misure adottate per scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione	*Descrizione*
Classificazione della violazione e motivazioni	*Descrizione*
Notificazione del Data Breach all'Autorità Garante	Si/NO Se sì, notificato in data: Dettagli:
Comunicazione del Data Breach agli interessati	Si/NO Se sì, notificato in data: Dettagli:
Comunicazione del Data Breach ad altri soggetti	Si/NO Se sì, notificato in data: Dettagli: