Università degli Studi di Perugia

Segnalazione delle Violazioni di Dati personali (Data breach)

Sommario

1. Perché segnalare una violazione dei dati personali?

Una violazione di dati personali può avere come conseguenza danni fisici, materiali o immateriali sulle persone cui si riferiscono i dati, tra cui violazioni di diritti, discriminazioni, pregiudizi, furto d'identità o perdite economiche, danni derivanti dalla perdita di controllo dei dati o dal loro illecito utilizzo.

Chiunque viene a conoscenza di un incidente di sicurezza che comporti, o possa comportare, una violazione di dati personali trattati in Ateneo **deve subito procedere** ad effettuare la segnalazione, come nel seguito descritto. La tempestività è fondamentale per minimizzare l'impatto della violazione sugli interessati (persone alle quali i dati si riferiscono) e prevenire situazioni nelle quali la stessa possa ripresentarsi.

2. Cos'è una violazione di dati personali?

La violazione dei dati personali, o Data Breach, è definita come "la 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".

Nello specifico:

- La **distruzione,** comporta che i dati non esistono più o sono in una forma inutilizzabile per l'Ateneo o per chi deve disporne legittimamente.
- La **modifica,** rappresenta un evento a seguito del quale i dati risultano alterati, corrotti o incompleti.
- La **perdita,** costituisce una condizione in cui i dati esistono ancora, ma chi è legittimato ad utilizzarli non ne ha più il controllo o l'accesso, ovvero non ha più i dati.
- La **divulgazione,** espone i dati al pubblico o all'accesso da parte di un numero indefinito di destinatari, non autorizzati a conoscerli o trattarli, perdendone il controllo.
- L'**accesso**, consente l'acquisizione del contenuto informativo dei dati, in una qualsiasi delle fasi di trattamento (raccolta, memorizzazione, transito su rete trasmissiva, comunicazione, condivisione, archiviazione, ….) da parte di soggetti non a ciò autorizzati.

Per le definizioni qui utilizzate, si rimanda all'art. 3 del Regolamento sul trattamento dei dati personali di Ateneo o all'art. 4 del Regolamento UE 2016/679 o GDPR.

3. Alcuni esempi di violazioni di dati personali e loro classificazioni

Le violazioni di dati personali o *data breach* si classificano come:

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 modificato in modo accidentale o non autorizzato;
c) **violazione della disponibilità**: quando in modo accidentale, o per dolo, non si consente a chi è autorizzato di accedere ai dati o i dati sono stati distrutti.

Una violazione di dati personali può rientrare in una o più categorie. Di seguito vengono proposti alcuni casi di data breach a titolo esemplificativo e non esaustivo: in caso di dubbi nell'individuazione di un evento come violazione di dati personali, esporre il caso scrivendo a rpd@unipg.it

Tipologia di *Data Breach*	Esempio e entità del rischio correlato
violazione della disponibilità	Si è verificato il furto o lo smarrimento di una Chiavetta USB o Notebook o Tablet o Smartphone o Hard Disk su cui sono memorizzati dati personali o è possibile accedervi. Il rischio è alto se i dati **non sono cifrati** o sono cifrati con algoritmi obsoleti, di cui sono note le vulnerabilità
violazione della riservatezza	C'è il ragionevole sospetto che qualcuno ha avuto accesso a dati personali, non essendo a ciò autorizzato, o che i dati siano stati consultati e/o sottratti impropriamente (dati gestiti in applicativi dell'Università, file presenti su pc o altri dispositivi, elenchi allegati ad e-mail, o contenuti in essa, ...)
violazione della riservatezza e della disponibilità	Una postazione di lavoro, o un server vengono compromessi da un Ransomware e conseguentemente i dati vengono cifrati. Il rischio è alto se non esiste un BackUp dei dati e/o c'è una ragionevole evidenza che i dati personali possono essere stati esfiltrati dal dispositivo. La violazione sussiste comunque, con rischi meno gravi, se esiste un back up dei dati che consente un ripristino in tempi ragionevoli, e c'è una ragionevole evidenza che i dati personali **non** sono stati sottratti dal dispositivo
violazione della riservatezza	Sono state compromesse le credenziali di accesso alla posta elettronica, ad uno o più sistemi informatici che trattano dati personali, ad esempio per aver dato seguito ad un messaggio di *phishing*
violazione della riservatezza	A seguito di un errore di programmazione e configurazione di un sistema informatico o di una applicazione informatica, sono stati resi accessibili dati personali a soggetti non autorizzati al trattamento o diversi dai diretti Interessati
violazione della riservatezza	Sono stati comunicati dati personali ad errato destinatario (ad esempio per invio ad indirizzo email errato) o pubblicati on line dati personali che non dovevano essere diffusi
violazione della riservatezza	Sono stati inviati ad una mailing list uno o più messaggi con numerosi indirizzi email privati dei destinatari in chiaro, nel campo 'A' o nel campo 'CC' (in tali casi vanno inseriti in 'ccn')
violazione dell'integrità	Sono stati utilizzati dati personali non aggiornati o non verificati, con danni sugli interessati (p.e. per il calcolo degli emolumenti, le agevolazioni agli studenti, per le graduatorie d'accesso ai corsi a numero chiuso,..)

Anche l'accesso abusivo, inteso come accesso ai sistemi informatici o cartelle dati ai quali non si è autorizzati, o ad informazioni personali che non potevano essere accedute, specie se con successivo utilizzo personale delle informazioni illecitamente acquisite, si configura come data breach.

4. Segnalazione di una violazione di dati personali, anche potenziale

"Abboccare" ad un phishing delle nostre credenziali di Ateneo (o di un altro sito, dove però avevamo scelto la stessa password), trovare on line documenti riconducibili al contesto universitario, contenenti dati personali che non dovrebbero essere pubblici, smarrire un fascicolo del personale o il cellulare, da cui si può accedere alla posta elettronica o al protocollo di ateneo, comprendere che un sistema informatico tratta dati eccedenti gli scopi ai quali è finalizzato, conoscere prassi scorrette di utilizzo e conservazione di documenti cartacei che consentono a persone non autorizzate di conoscerne il contenuto … sono tutti esempi, non esaustivi, di situazioni che devono essere segnalate all'Ateneo, per consentirne la valutazione e, se del caso, evitarne il ripetersi e limitare i danni.

Cosa devi segnalare?	
Qualsiasi informazione utile a chi prenderà in carico la segnalazione, per comprendere l'entità del problema, incluso un contatto per essere richiamati in caso di necessità. Alla pagina https://www.unipg.it/ateneo/protezione-dati-personali/segnalazione-violazioni è presente un modulo scaricabile, utilizzabile per la segnalazione, i cui contenuti richiesti sono almeno quelli di seguito riportati	
1	I tuoi dati di contatto, perché effettui la segnalazione e potrebbero servire ulteriori dettagli dell'evento
2	Quando è avvenuta la violazione o quando sei venuto a conoscenza della violazione
3	Le possibili cause della violazione, se anche delle proprie credenziali, di dati personali suoi o di terzi
4	La tipologia dei dati coinvolti (generici, sanitari, bancari, documenti di identità,…) e le categorie delle persone cui si riferiscono (dipendenti, studenti, fornitori, volontari sottoposti a ricerca,…)
6	Il tipo di violazione sui dati (rif. par. 3 precedente)
7	La numerosità dei dati personali violati, anche solo per fascia numerica
8	Se, ove possibile, hai già provveduto ad azioni per limitare i danni e se si, quali (in caso di phishing, ad esempio, hai cambiato la password)

Chi deve segnalare, in che modo e quando?	
Chi deve segnalare?	Chiunque tra docenti, personale, collaboratori, fornitori, responsabili del trattamento, studenti, utenti esterni, etc. che sia a conoscenza di una violazione o abbia dubbi in merito
In che modo?	Utilizzando la modalità più rapida tra: • e-mail:comunicazione.violazione@unipg.it • ticket: https://www.helpdesk.unipg.it/ • telefonicamente (solo orari ufficio): ai numeri riportati in fondo alla pagina https://www.unipg.it/ateneo/protezione-dati-personali/segnalazione-violazioni
Quando?	Appena hai il sospetto o ne vieni a conoscenza

Ricorda che è sempre buona regola:

- *scegliere password complesse e diverse per le credenziali di ateneo, altri servizi (p.e home banking) e social;*
- *proteggere con password, o altri meccanismi di autenticazione forte, i dispositivi personali e di lavoro da cui sia possibile accedere ai servizi di ateneo (posta, area riservata, protocollo, U-Gov,..). In caso di furto o perdita rendi così difficile lo sblocco del dispositivo e hai il tempo di cambiare subito le password e comunicare l'incidente per limitare i danni;*
- *non memorizzare le password nei singoli servizi (scegli sempre "non salvare" o "non salvare mai per questo sito") e, per ricordarle, utilizza p.e. una frase da cui derivarle;*
- *utilizzare solo un Gestore password sicuro, se si vogliono memorizzare le password sul dispositivo, in un file dedicato (mai conservarle in chiaro).*

Ulteriori indicazioni le trovi alla pagina https://www.unipg.it/ateneo/protezione-dati-personali/segnalazione-violazioni. In caso di dubbi o domande, visita le FAQ all'indirizzo https://www.unipg.it/ateneo/protezione-dati-personali/faq o scrivi a rpd@unipg.it