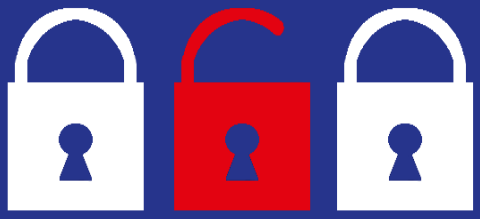
A.D. 1308
unipg
UNIVERSITÀ DEGLI STUDI
DI PERUGIA



Segnalazione violazioni di dati personali (Data breach)

SOMMARIO

PERCHÉ È NECESSARIO SEGNALARE UNA VIOLAZIONE DI DATI PERSONALI?

I dati di una carta di credito, un documento d'identità elettronico, le credenziali d'accesso ad un qualsiasi servizio on line, i recapiti privati o i dati curricolari dei dipendenti o degli studenti, costituiscono esempi di dati personali, come anche i dati personali raccolti o trattati per finalità di ricerca.

Il loro utilizzo ha effetti di notevole utilità per le persone cui si riferiscono, soprattutto nell'ambito dei servizi digitali e delle comunicazioni elettroniche e, nel caso della ricerca, concorrono a scoperte importanti e di interesse collettivo.

Quando invece i dati personali entrano nella disponibilità di terzi non autorizzati, possono esserci effetti negativi significativi sulla vita delle persone, tra cui danni fisici, materiali o immateriali, pregiudizi alla reputazione e danni economici o sociali.

Per questo motivo è di fondamentale importanza che una violazione, anche presunta, di dati personali trattati in Università, sia segnalata tempestivamente da chiunque ne venga a conoscenza e, in base all'art. 33 Regolamento UE 2016/679, è un obbligo per l'Università prenderla in carico e gestirla nel minor tempo possibile.

La tempestività infatti può:

- evitare o ridurre i rischi per i diritti e le libertà degli interessati;
- evitare o ridurre i danni economici per l'interessato e per l'Ateneo;
- evitare all'Ateneo di incorrere nelle sanzioni previste dalla normativa europea, per omessa notifica all'Autorità garante e agli interessati, qualora dovuta;
- minimizzare l'impatto della violazione sui sistemi di Ateneo e prevenire che si ripeta.

COS'È UNA VIOLAZIONE DI DATI PERSONALI?

Una violazione dei dati personali (nel seguito violazione o Data breach) è definita dal Regolamento UE 2016/679, o GDPR, come "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".

Si distingue tra:

- **Violazione della riservatezza**: quando si verifica un accesso accidentale o abusivo a dati personali, una comunicazione a soggetti non autorizzati a conoscerli o una divulgazione di dati non destinati a diffusione (p.e. tramite pubblicazione on line);
- **Violazione della disponibilità**: quando si verifica la perdita o distruzione accidentale, non autorizzata o dolosa del dato personale, o per l'indisponibilità prolungata dei dati a seguito di un incidente informatico o elettrico;
- **Violazione dell'integrità**: quando avviene un'alterazione accidentale, non autorizzata oppure dolosa del dato personale.

Una violazione di dati personali può comprendere uno o più di tali eventi.

IL FURTO DELLE CREDENZIALI UNICHE DI ATENEO

La perdita o la sottrazione illecita delle credenziali uniche di Ateneo tramite phishing, per esempio, è uno dei fenomeni più diffusi di violazione della riservatezza di dati personali. Essa richiede il cambio immediato della password per evitare violazioni ulteriori sui dati personali che, con tali credenziali, possono essere acceduti o comunque gestiti.

Più i dati personali acceduti tramite queste credenziali sono critici, per natura dei dati, tipologia di interessati, contesto di utilizzo e quantità, più è critica la loro violazione. Nel caso di progetti di ricerca, la violazione delle credenziali può comportare anche la perdita di parti del progetto con esse accessibili.

Una pagina del sito di Ateneo sulla sicurezza on line è stata dedicata a questo caso e un apposito modello di segnalazione è stato reso disponibile alla pagina Segnalazione violazioni - Università degli Studi di Perugia (unipg.it).

ALTRI ESEMPI DI VIOLAZIONI

a. La divulgazione di dati personali presenti in documenti, senza che vi sia un obbligo di legge alla diffusione, con qualsiasi mezzo venga effettuata (canali social, pubblicazione sul sito di Ateneo…). Per ulteriori indicazioni vedasi le "Linee guida per la pubblicazione di atti e documenti contenenti dati personali" adottate dall'Ateneo;
b. La perdita o furto di strumenti, anche personali, nei quali sono memorizzati dati utilizzati per lavoro o da cui è possibile accedervi;
c. La perdita o il furto di fascicoli cartacei;
d. L' infedeltà aziendale (ad esempio: una persona interna che, avendo autorizzazione ad accedere ai dati, ne produce una copia ad uso personale o li distrugge intenzionalmente);
e. L'accesso abusivo ai dati (ad esempio: accesso non autorizzato ad un sistema informatico o ad una parte di dati con esso gestiti, utilizzando credenziali sottratte ad un collega);
f. I casi di pirateria informatica (introduzione di virus tramite apertura di file provenienti da mittenti non verificati o altri attacchi alla rete aziendale);
g. Le violazioni di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o armadi contenenti archivi con informazioni riservate);
h. L'invio di e-mail contenenti dati personali e/o particolari ad uno o più destinatari errati.

DIZIONARIO PER LA SEGNALAZIONE

1. **accesso:** accesso non autorizzato ai dati da parte di soggetti, interni o esterni, non aventi diritto a ciò;
2. **banca dati:** qualsiasi complesso organizzato di dati personali;
3. **comunicazione:** comunicazione (fortuita o intenzionale) dei dati verso terzi non autorizzati;
4. **dato personale**: 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;

5. **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. È irreversibile;
6. **divulgazione dei dati**: condizione in cui i dati sono oggetto di divulgazione (conoscibilità impropria di informazioni ad ampia platea) o accesso da parte di destinatari non autorizzati, o altra forma di trattamento effettuato in violazione del GDPR;
7. **incidente di sicurezza:** evento o serie di eventi sulla sicurezza delle informazioni, indesiderati o imprevisti, che hanno una significativa probabilità di minacciare la sicurezza delle informazioni, oltre a compromettere le operazioni aziendali;
8. **modifica dei dati**: condizione (accidentale o intenzionale) in cui i dati risultano alterati, corrotti o incompleti;
9. **perdita dei dati**: condizione in cui i dati esistono ancora ma il Titolare non ne ha più il controllo o l'accesso (indisponibilità temporanea dei dati) ovvero il Titolare non ha più i dati;
10. **RPD o DPO**: il Responsabile per la Protezione dei dati di Ateneo;
11. **Titolare**: il Titolare del trattamento. In questo contesto è l'Università degli studi di Perugia.

Altre definizioni sono all'art. 3 del Regolamento per il trattamento dei dati personali Unipg

CHI È TENUTO A SEGNALARE?

A prescindere dalla tipologia di rapporto contrattuale intercorrente con l'Ateneo, chiunque sia a conoscenza di violazioni concrete, potenziali o anche solo sospette di dati personali, trattati dall'Università nel corso delle prestazioni svolte, è tenuto a segnalare tempestivamente l'evento, per limitarne gli effetti sugli interessati.

Tra essi sono ad esempio incluse tutte le persone (fisiche o giuridiche) che accedono ai suddetti dati per l'esecuzione delle prestazioni di lavoro, per adempimenti normativi o per attività contrattualizzate, inclusi coloro che trattano dati personali per conto dell'Università (Responsabili del trattamento - art. 28 Regolamento UE 2016/679 o GDPR).

È opportuno e auspicabile che provveda alla segnalazione anche qualsiasi persona esterna all'Ateneo, che sia venuta accidentalmente a conoscenza di violazioni, anche presunte, di dati personali trattati dall'Università.

QUALI SONO LE VIOLAZIONI DA SEGNALARE?

La segnalazione deve riferirsi a violazioni, anche solo sospette, di dati personali conservati o trattati dall'Università o per conto dell'Università per una finalità istituzionale e:

- con uno o più di questi mezzi:
  - strumenti e sistemi utilizzati in Ateneo;
  - dispositivi personali (smartphone o altri);
  - tramite fornitori esterni di servizi in rete (compresi i cd. "servizi cloud");
- in qualsiasi formato (inclusi documenti cartacei).

Nel caso di trattamenti di dati attraverso servizi esternalizzati, le strutture, competenti per l'affidamento del servizio devono procedere alla nomina dei Responsabili del trattamento di dati (come richiesto dall'art. 28 GDPR), secondo il fac-simile predisposto e pubblicato nell'Area riservata del sito di Ateneo.

COME SEGNALARE?

La segnalazione va indirizzata preferibilmente via e-mail, all'indirizzo comunicazione.violazione@unipg.it. Schematicamente:

Chi deve farla	**Chiunque** ne venga a conoscenza (in dettaglio vedi il precedente paragrafo "A chi si rivolge questa procedura")
Quando	Appena ne viene a conoscenza o ha un ragionevole sospetto di una violazione di dati personali, trattati per finalità istituzionali
Come (in ordine di priorità e in alternativa)	• e-mail all'indirizzo comunicazione.violazione@unipg.it • inserimento segnalazione al servizio di ticketing: https://www.helpdesk.unipg.it/open.php (utilizzando l'argomento "Violazione Dati Personali") • contatto telefonico allo 075 5851 • di persona, al proprio responsabile o al Responsabile protezione dati personali, che provvederà ad informarne il Gruppo di risposta agli eventi (GRE) in ogni caso, scegliendo la via più breve, anche in base alla segnalazione da effettuare, alla fascia oraria o agli strumenti disponibili. Altre info utili sono pubblicate alla pagina: Segnalazione violazioni - Università degli Studi di Perugia (unipg.it)
Cosa comunicare	• i propri dati di contatto (per approfondire la segnalazione) • una descrizione dell'evento, quanto più possibile dettagliata circa la natura dell'evento, i dati coinvolti, le modalità e la data/ora di conoscenza...
Risultato atteso di questa fase	Presa in carico della segnalazione da parte del Gruppo di Risposta agli Eventi e, in caso di violazione conclamata, avvio tempestivo delle fasi di analisi, di contenimento e degli adempimenti di legge.

COSA AVVIENE DOPO LA SEGNALAZIONE?

L'Università ha istituito un GRE (Gruppo di risposta agli eventi) che ha, al suo interno, un nucleo di coordinamento.

Questo nucleo, ricevuta una segnalazione di violazione o sospetta violazione dei dati personali, ha il compito di attivarsi prontamente per analizzarla. In caso di conferma del data breach, coinvolge altri membri del GRE per le attività necessarie a contenerne gli effetti, valutarne la gravità e le conseguenze per gli interessati e, nei casi di media/alta gravità, collaborare con il Rettore per gli adempimenti richiesti dal Regolamento UE 2016/679 GDPR (notifica al Garante privacy e agli interessati, se dovuta).

Tutta la comunità accademica è tenuta a collaborare, fornendo tempestivamente al GRE ogni informazione richiesta, affinché possa svolgere al meglio i suoi compiti.

RACCOLTA E ANALISI DELLA POTENZIALE VIOLAZIONE

<table>
<tr><td>Chi deve farla</td><td colspan="3">Il GRE, attraverso il suo nucleo di coordinamento. Collaborano:
Il soggetto segnalante
i Responsabili delle strutture interessate dall’evento segnalato
altri soggetti a conoscenza di elementi utili all’analisi (ad esempio il personale dei Servizi Informatici di Ateneo, il referente contrattuale del servizio esterno coinvolto nella violazione, etc…)</td></tr>
<tr><td>Quando</td><td colspan="3">Appena ricevuta la segnalazione</td></tr>
<tr><td>Come</td><td colspan="3">Raccogliendo, nel più breve tempo possibile, altre informazioni necessarie per la comprensione della portata dell’evento, con l’ausilio di modelli di raccolta delle informazioni occorrenti eventualmente anche in più fasi successive</td></tr>
<tr><td rowspan="5">Risultato atteso di questa fase (max 12h)</td><td colspan="3">La segnalazione costituisce una violazione di dati personali di cui è Titolare l’Università?</td></tr>
<tr><td>SI</td><td colspan="2">NO</td></tr>
<tr><td>Analisi e quantificazione della gravità dell’evento segnalato, tramite ulteriore raccolta di informazioni. La comunità accademica è tenuta a collaborare con priorità assoluta</td><td colspan="2">Riguarda dati gestiti dall’Università per conto di partner o altri soggetti?</td></tr>
<tr><td rowspan="3">Attivazione delle prime azioni di contenimento (es. cambio dei codici di accesso, riparazione fisica di strumentazione, utilizzo dei file di back up per recuperare dati persi o danneggiati, isolamento/chiusura di un settore compromesso della rete, etc.)</td><td>SI</td><td>NO</td></tr>
<tr><td rowspan="2">L’Università è tenuta a comunicare quanto prima al Titolare (rappresentante legale del partner o di altri soggetti), attraverso il referente del contratto, l’analisi svolta</td><td rowspan="2">Archiviazione</td></tr>
<tr><td>Verbalizzazione delle attività svolte e inserimento nel Registro degli incidenti</td></tr>
<tr><td colspan="2">Avvio delle azioni successive, anche per gli adempimenti normativamente richiesti</td></tr>
</table>

AZIONI DI CONTENIMENTO E ADEMPIMENTI DI LEGGE

Chi deve farla	Il **GRE**, con la collaborazione di chiunque possa a ciò contribuire
Quando	Da quando è pervenuta la segnalazione fino a che si è risolta, sempre ottimizzando i tempi di intervento. Il GRE supporta il Titolare sia nella notifica all’Autorità Garante, che va effettuata entro le 72h da quando si è constatata la violazione di dati personali, sia nella comunicazione agli interessati, se dovute.

<table>
<tr><td>Come</td><td colspan="4">Eseguendo la valutazione della gravità della violazione e definendo un piano di interventi, in base al contesto dell’evento e ai dati raccolti.

Il GRE ne informa il Rettore, il Direttore generale e il Delegato per l’area legale, per le decisioni strategiche da assumere.</td></tr>
<tr><td rowspan="11">Risultato atteso di questa fase</td><td colspan="4">Valutazione del livello di impatto potenziale sui diritti e sulle libertà delle persone fisiche e della probabilità che tale impatto si verifichi</td></tr>
<tr><td>Non c’è rischio</td><td>Rischio Basso</td><td>Rischio Medio</td><td>Rischio Alto/Molto alto</td></tr>
<tr><td rowspan="10">Chiusura dell’evento e inserimento nel Registro degli incidenti, indicando le motivazioni del non luogo a procedere</td><td colspan="3">Inserimento nel Registro degli incidenti e inizio della redazione del Piano rimediale</td></tr>
<tr><td colspan="3">Attuazione azioni che possano limitare i danni che la violazione potrebbe causare e verifica della loro attuazione (di concerto con i responsabili delle strutture interessati dall’incidente di sicurezza e, se del caso, con la Polizia postale e l’Autorità Garante)</td></tr>
<tr><td>Rischio Basso</td><td>Rischio Medio</td><td>Rischio Alto/Molto Alto</td></tr>
<tr><td rowspan="2">Chiusura della violazione Inserimento nel Registro degli incidenti, indicando le motivazioni per cui si è deciso di non procedere con la notifica al Garante e agli interessati</td><td colspan="2">Entro 72 ore notificare la violazione all’Autorità Garante per la Protezione dei dati personali</td></tr>
<tr><td>-</td><td>(rischio alto/molto alto) Entro 72 ore o immediatamente dopo, comunicare la violazione agli interessati</td></tr>
<tr><td rowspan="2">-</td><td colspan="2">Attività varie conseguenti ad una violazione con impatto rilevante</td></tr>
<tr><td colspan="2">Chiusura dell’evento e aggiornamento del Registro degli incidenti, indicando dettagliatamente quanto successo. Redazione di relazione completa</td></tr>
<tr><td colspan="4">Analisi post evento ed eventuali suggerimenti e individuazione di misure precauzionali al fine di evitare il ripetersi di analoghi incidenti di sicurezza</td></tr>
</table>