AREA AFFARI GENERALI E LEGALI
SETTORE CONSULENZA

UNIVERSITÀ DEGLI STUDI DI PADOVA

Ultimo aggiornamento: 23/12/2012

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH)

Abbreviazioni e acronimi

- *Data breach* = violazione di dati personali
- *DPO* = Data protection officer (Responsabile della protezione dei dati personali)
- *Garante privacy* = Garante per la protezione dei dati personali
- *GDPR* = Regolamento generale sulla protezione dei dati (Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)
- *RTD* = Responsabile per la transizione digitale
- *Team di risposta* = gruppo di supporto per la gestione delle segnalazioni delle violazioni dei dati, composto dal DPO, RTD e loro collaboratori preventivamente incaricati al presidio dell'indirizzo violazioni.dati@unipd.it e alla valutazione delle segnalazioni
- *Università* = Università degli Studi di Padova

AMBITO DI APPLICAZIONE E DESTINATARI

1. Violazione di dati personali (*data breach*): definizione e caratteristiche

Per violazione di dati personali (o *data breach*) si intende *"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"* (art. 4, punto12 del GDPR).

Di conseguenza, si applica la procedura di segnalazione delle violazioni esclusivamente quando un incidente di sicurezza comporta la violazione anche di **dati *"personali"***, ossia una violazione che può compromettere la capacità dell'Università di garantire il rispetto dei principi applicabili al trattamento dei dati personali, ai sensi dell'art. 5 GDPR («liceità, correttezza e trasparenza», «limitazione della finalità», «minimizzazione dei dati», «esattezza», «limitazione della conservazione», «integrità e riservatezza»).

Si possono distinguere tre tipi di violazioni di dati personali:

- **violazione di riservatezza**, quando si verifica una divulgazione o l'accesso a dati personali non autorizzato o accidentale;
- **violazione di integrità**, quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
- **violazione della disponibilità anche temporanea**, quando si verifica la perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

2. Finalità e destinatari della procedura di gestione delle violazioni di dati personali

La presente procedura è diretta a garantire la capacità dell'Università di rilevare e limitare **tempestivamente** gli effetti di una violazione di dati personali, valutare il rischio per le persone fisiche, e stabilire se sia necessario notificare la violazione al Garante privacy e comunicarla alle persone fisiche interessate, ai sensi degli artt. 33 e 34 del GDPR.

La mancata segnalazione di una violazione a una persona fisica o all'autorità di controllo può comportare l'imposizione di una sanzione all'Università ai sensi dell'articolo 83 del GDPR.

Il mancato rispetto della presente procedura può 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.

2.1. A chi sono rivolte le procedure di segnalazione?

Queste procedure sono rivolte a tutti i soggetti che, a qualsiasi titolo, trattano dati personali di cui l'Università è titolare o responsabile ai sensi del GDPR:

a) *Destinatari interni*: i lavoratori dipendenti e collaboratori che a qualsiasi titolo, e quindi a prescindere dal tipo di rapporto contrattuale, hanno accesso ai dati personali trattati nel corso delle prestazioni erogate *da* o *per conto* dell'Università;

b) *Soggetti esterni:* qualsiasi soggetto (persona fisica o persona giuridica) che, in ragione del rapporto contrattuale in essere con l'Università, ha accesso a dati personali di cui l'Università è titolare e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare del trattamento.

2.2. A quali tipi di dati personali si riferisce questa procedura?

Questa procedura si applica quando sono violati i seguenti dati personali:

a) dati personali trattati *da* e *per conto* dell'Università, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;

b) dati personali conservati o trattati a mezzo di qualsiasi sistema o software 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 (art. 4, punto 1, GDPR).

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI

L'Università è tenuta, **entro 72 ore dalla conoscenza di una violazione di dati personali** che presenti un rischio per i diritti e le libertà degli interessati, alla notifica al Garante e, in caso di accertata elevata gravità del rischio, alla comunicazione agli interessati.

Le informazioni relative all'incidente devono essere raccolte e trasmesse al più presto all'indirizzo violazioni.dati@unipd.it.

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. La valutazione d'impatto sarà integrata con le informazioni che vengono acquisite nella prosecuzione dell'indagine.

1. Procedura interna di rilevazione e segnalazione di una potenziale violazione

Per garantire il rispetto dei tempi di risposta imposti dal GDPR (72 ore), è necessario segnalare al team di risposta (violazioni.dati@unipd.it) **immediatamente**, e comunque **non oltre 8 ore dall'avvenuta conoscenza** di un incidente di sicurezza, un'eventuale violazione dei dati personali trattati dall'Università.

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**.

È opportuno segnalare qualsiasi tipo di incidente di sicurezza, anche lieve e connesso ai dati personali, per consentire di valutare la gravità e le conseguenze per gli interessati e aggiornare il "Registro delle violazioni dei dati", che permette una costante analisi del rischio e di predisporre adeguate misure di prevenzione.

1.1. Rilevazione di un incidente di sicurezza

Chi	Chiunque ne venga a conoscenza (soggetti autorizzati, personale, collaboratori, fornitori, Responsabile del trattamento, utenti esterni, DPO)
A chi	Responsabile di struttura (dirigente, direttore di dipartimento o centro) Referente privacy (SD, RTG, direttore d'ufficio, responsabile di settore, responsabile del progetto di ricerca)
Quando	Immediatamente
Come	Comunicando l'incidente di sicurezza al Responsabile di struttura e al Referente privacy, anche per le vie brevi (telefonicamente, di persona, via e-mail)

Ogni dipendente, collaboratore o collaboratrice che a qualsiasi titolo ha accesso ai dati personali trattati "da" o "per conto" dell'Università, deve individuare e segnalare **immediatamente** al responsabile della propria struttura e al referente organizzativo privacy, una violazione dei dati (anche se solo sospetta), che abbia colpito il suo sistema o il suo ufficio.

È opportuno segnalare qualsiasi tipo di incidente di sicurezza, anche lieve e connesso ai dati personali, per consentirne la gestione e valutare la gravità e le conseguenze per gli interessati. Ciò consentirà all'Ateneo di mantenere un registro degli incidenti aggiornato, che permette una costante analisi del rischio e di predisporre adeguate misure di prevenzione.

Nel caso in cui il computer fisso, il pc portatile, hard disk, chiavette USB o altri supporti di memoria fossero oggetto di furto o smarrimento, occorre segnalare immediatamente l'avvenimento.

Vanno segnalati anche tutti gli incidenti comunque correlati ai dati personali, quali furto di informazioni effettuate online, cancellazione accidentale di informazioni, comunicazione di informazioni a terzi per errore. Ciò anche se non vi è stato un comportamento intenzionale alla base, ma un evento accidentale.

Va inteso come *data breach* anche un attacco di *phishing* andato a buon fine, ossia l'aver fornito o diffuso credenziali e dati tecnici a un soggetto terzo.

Esempi di violazioni di dati personali

In generale, integra un'ipotesi di violazione dei dati personali qualsiasi situazione che può portare un soggetto non autorizzato alla conoscenza o disponibilità di dati personali. A titolo meramente esemplificativo, si è in presenza di una violazione di dati personali nei seguenti casi:

a) divulgazione non autorizzata di dati confidenziali a persone non autorizzate;
b) divulgazione al pubblico di dati riservati;
c) accesso o acquisizione dei dati da parte di terzi non autorizzati;
d) invio accidentale di e-mail contenenti dati personali o particolari al destinatario sbagliato;
e) violazione di misure di sicurezza fisiche quali ad esempio la forzatura di porte o di finestre di particolari locali (sale macchine, depositi dei nastri di backup, locale che ospita il server, archivi anche cartacei, locali contenenti informazioni riservate);
f) perdita o furto di documenti cartacei;
g) furto o smarrimento di un computer o dispositivo portatile, disco rimovibile, pen drive usb, perdita di dispositivi informatici contenenti dati personali;
h) virus o altri attacchi al sistema informatico o alla rete di Ateneo;
i) deliberata alterazione di dati personali;
j) impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware;
k) perdita o distruzione accidentale di dati personali o a causa di incidenti, eventi avversi, incendi o altre calamità.

1.2. Valutazione delle possibili conseguenze e contromisure

Chi	Responsabile di struttura (dirigente, direttore di dipartimento o centro) Referente privacy (SD, RTG, direttore d'ufficio, responsabile di settore, responsabile del progetto di ricerca)
Quando	Immediatamente dopo la ricezione della segnalazione
Come	Coordinando la raccolta delle informazioni, eventualmente con il supporto degli amministratori di sistema della struttura

Appena riceve una segnalazione, il Responsabile della struttura, anche tramite i referenti privacy coinvolti e, se necessario, con supporto degli amministratori di sistema competenti, deve:

a) coordinare la raccolta delle informazioni nel più breve tempo possibile;
b) valutare se si tratta di una violazione di dati "personali";
c) disporre l'adozione delle contromisure necessarie per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi;
d) trasmettere il modello per la segnalazione delle violazioni a violazioni.dati@unipd.it (vedi prossimo paragrafo).

1.3. Segnalazione al *Team di risposta* (violazioni.dati@unipd.it)

Chi	Responsabile di struttura (dirigente, direttore di dipartimento o centro) Referente privacy (SD, RTG, direttore d'ufficio, responsabile di settore, responsabile del progetto di ricerca)
A chi	Team di risposta (DPO, RTD e collaboratori)
Quando	Immediatamente e comunque **non oltre 8 ore** dalla conoscenza dell'evento
Come	Inviando il *"Modulo per la segnalazione di violazioni di dati personali"* (allegato 1) a violazioni.dati@unipd.it

Se l'incidente di sicurezza ha comportato la violazione di dati "personali", il responsabile della struttura e i referenti organizzativi privacy devono fornire tempestivamente informazioni più dettagliate possibile su ciò che è accaduto, compilando l'apposito **modulo di segnalazione** pubblicato nella sezione dedicata del portale di Ateneo (**Allegato 1**).

Il modulo compilato, **entro 8 ore** lavorative dall'avvenuta conoscenza dell'evento, deve essere trasmesso al team di risposta all'indirizzo violazioni.dati@unipd.it.

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**.

Le informazioni più importanti sono:

A. tipo di dati violati;
B. dati particolari (ex sensibili) eventualmente violati;
C. numero di soggetti coinvolti;
D. soggetti minori eventualmente coinvolti;
E. estensione dell'incidente di sicurezza;
F. periodo temporale dell'incidente;
G. misure di sicurezza adottate;
H. cifratura o meno dei dati violati.

2. Gestione della segnalazione da parte del team di risposta

Il Direttore generale, su proposta del DPO e del RTD, individua un gruppo di supporto per la gestione delle segnalazioni delle violazioni dei dati denominato "team di risposta" e composto dal DPO, dal RTD e da loro collaboratori preventivamente incaricati al presidio dell'indirizzo violazioni.dati@unipd.it.

Il team di risposta, in collaborazione con i soggetti segnalanti, i responsabili e i referenti privacy delle relative strutture, procede senza indugio a:

1. Valutare l'impatto dell'incidente di sicurezza
2. Individuare le possibili contromisure
3. Notificare la violazione al Garante (se necessario)

4. Comunicare la violazione agli interessati coinvolti (se necessario)
5. Aggiornare il Registro delle violazioni dei dati personali

2.1. Valutazione d'impatto dell'incidente di sicurezza

Chi	DPO e team di risposta, in collaborazione con il responsabile e i referenti privacy della struttura
Quando	Immediatamente, appena ricevuta la segnalazione
Come	Valutando il **rischio** [= gravità *x* probabilità] dell'impatto della violazione sui diritti degli interessati, in base a parametri predeterminati

L'Università, per mezzo del DPO e del team di risposta, in collaborazione con i soggetti segnalanti e coinvolti dall'incidente di sicurezza, valuta l'impatto della violazione dei dati personali per i diritti e le libertà delle persone fisiche, al fine di stabilire il **rischio** *[= gravità x probabilità]* e le **conseguenti azioni** che deve intraprendere:

a) adozione di misure per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi
b) notifica della violazione al Garante privacy, a meno che sia improbabile un rischio per i diritti e le libertà delle persone fisiche;
c) comunicazione agli interessati, se il rischio è elevato *[gravità x probabilità]*^{n}.

La tabella seguente presenta i principali fattori che devono essere considerati nella valutazione di impatto della gravità di una violazione sulla base delle informazioni raccolte.

FATTORI DA CONSIDERARE PER LA VALUTAZIONE D'IMPATTO DELLA VIOLAZIONE	
Gravità e probabilità	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	Divulgazione, Distruzione e Modifica, Perdita
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
Caratteristiche particolari dell'interessato	La violazione coinvolge in particolare dati personali di minori o altre persone fisiche vulnerabili
Numero di persone fisiche coinvolte	Numero di persone fisiche coinvolte nella violazione

2.2. Adozione di contromisure e azioni correttive

Chi	DPO e team di risposta
Quando	Contestualmente alla valutazione di impatto
Come	in collaborazione con il responsabile della struttura, i referenti privacy e gli amministratori di sistema delle strutture coinvolte

Il team di risposta, in collaborazione con il responsabile, i referenti privacy e gli amministratori di sistema delle strutture coinvolte individua le misure che possono essere adottate per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

La tempestività dell'adozione delle contromisure **può ridurre il rischio** per i diritti e le libertà degli interessati, facendo venir meno l'obbligo di notifica al Garante privacy o di comunicazione agli interessati (vedi prossimi paragrafi).

2.3. Notifica della violazione al Garante (se necessario)

Chi	Direttore generale, sentito DPO
A chi	Garante per la protezione dei dati personali
Quando	senza ingiustificato ritardo → necessità di motivazione se la notifica non avviene **entro 72 ore dalla conoscenza** della violazione
Come	Inviando il Modello notifica data breach compilato a *protocollo@pec.gpdp.it*

Se la violazione dei dati personali rappresenta un **rischio** per i diritti e le libertà delle persone fisiche, **il Direttore generale, sentito il DPO**, deve notificare il modulo compilato al Garante privacy tramite posta elettronica certificata all'indirizzo *protocollo@pec.gpdp.it* e deve essere sottoscritta digitalmente.

La notifica al Garante deve essere effettuata dal titolare del trattamento senza ingiustificato ritardo e, ove possibile, **entro 72 ore dalla conoscenza** della violazione, con le modalità di cui all'art. 65 del d.lgs. 7 marzo 2005, n. 82 (recante il «Codice dell'amministrazione digitale»), mediante i sistemi telematici indicati nel sito istituzionale del Garante. L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "NOTIFICA VIOLAZIONE DATI PERSONALI" e opzionalmente la denominazione del Università.

In caso di ritardo, è necessario motivare le **ragioni del ritardo** che hanno impedito la tempestività della notifica.

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**. La documentazione verrà integrata in un secondo momento, in collaborazione con il Garante privacy.

L'Università è tenuta a notificare la violazione dei dati personali al Garante con le modalità di cui all'art. 33 del Regolamento anche con riferimento al trattamento effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvo che il trattamento medesimo sia effettuato dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero (artt. 26 e 37, comma 6, del d.lgs. n. 51/2018).

2.4. Comunicazione agli interessati coinvolti (se necessario)

Chi	Responsabile della protezione dei dati (DPO)
A chi	Persone fisiche i cui dati personali sono stati violati (interessati)
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

Se la violazione dei dati presenta un **rischio "elevato"** per i diritti e le libertà delle persone fisiche, la comunicazione agli interessati deve essere fatta senza indugio. L'eventuale ritardo nella notificazione deve essere giustificato.

La comunicazione agli interessati deve contenere:

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

Se la segnalazione diretta agli interessati richiede uno sforzo ritenuto sproporzionato, è possibile utilizzare forme di comunicazione pubblica attraverso i canali istituzionali dell'Università, a condizione che questa modalità non rappresenti a sua volta un rischio per la protezione dei dati personali degli interessati.

2.5. Registro delle violazioni dei dati personali

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione o comunicazione della violazione di dati personali, il team di risposta documenta tutte le violazioni di dati personali, ai sensi dell'art. 33, par. 5, GDPR, annotandole nell'apposito Registro (allegato 2).

Il Registro delle violazioni dei dati contiene almeno le seguenti informazioni:

1. data e ora della violazione;
2. luogo della violazione (fisico o virtuale);
3. natura della violazione;
4. categorie di interessati coinvolti;
5. categorie di dati personali violati;
6. effetti della violazione;
7. contromisure adottate;
8. *se* è stata effettuata notifica all'Autorità Garante;
9. *se* è stata effettuata comunicazione agli interessati;
10. motivazione dei comportamenti adottati (valutazione d'impatto).

Il Registro data breach è continuamente aggiornato dal team di risposta coordinato dal DPO ed è messo a disposizione del *Garante per la protezione dei dati personali*, qualora ne faccia esplicita richiesta.