Procedura da adottare in caso di violazione dei dati personali

Art. 4, 33, 34 del Regolamento UE 679/2016

1. Premessa

Il presente documento è redatto in adempimento a quanto previsto dal Regolamento UE 679/2016 (GDPR) in materia di violazione dei dati personali.
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.
Il GDPR definisce violazione del dato personale o **DATA BREACH** ogni "violazione 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.

2. Scopo e ambito di applicazione

La presente procedura è predisposta al fine di tutelare le persone, i dati e le informazioni e documentare i flussi per la gestione delle violazioni dei dati personali trattati da Terre di Siena Lab, nella sua qualità di Titolare del trattamento.
La procedura definisce le modalità e le responsabilità per:
- identificare la violazione,
- analizzare le cause della violazione,
- definire le misure da adottare per rimediare alla violazione dei dati personali e attenuarne i possibili effetti negativi,
- registrare le informazioni relative alla violazione, le misure identificate e l'efficacia delle stesse,
- notificare una violazione di dati personali al Garante, nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche,
- comunicare una violazione dei dati personali all'interessato nel caso in cui il rischio fosse elevato.

La procedura si applica a qualunque attività svolta dal Titolare del trattamento con particolare riferimento a tutti gli archivi e/o documenti cartacei e a tutti i sistemi informativi attraverso cui sono trattati dati personali, anche con il supporto di fornitori esterni.
Terre di Siena Lab, quale Titolare del trattamento dei dati, ad integrazione delle procedure già adottate in materia di protezione dei dati personali, ha predisposto azioni da attuare nelle ipotesi in cui dovessero presentarsi violazioni concrete, potenziali o sospette di dati personali trattati da Terre di Siena Lab in qualità di Titolare, al fine di:
- evitare rischi per i diritti e le libertà degli interessati,
- evitare danni economici all'azienda,
- notificare la violazione (Data Breach) al Garante e/o agli interessati, nei tempi e

nei modi previsti dalla normativa di riferimento,
- non incorrere nelle sanzioni previste dal GDPR per omessa notifica,
- minimizzare l'impatto della violazione e prevenire che si ripeta.

3. Verso chi si rivolge la procedura

La procedura è rivolta a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento, in qualsiasi formato e con qualsiasi mezzo, quali:
• i dipendenti, nonché coloro che a qualsiasi titolo (a prescindere pertanto dal tipo di rapporto intercorrente con Terre di Siena Lab) abbiano accesso
ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento;
• qualsiasi soggetto (persona fisica o persona giuridica) 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 *ex* art. 28 GDPR o di autonomo Titolare.
Il rispetto della predisposta 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 le terze parti inadempienti, secondo le normative vigenti in materia.

4. La procedura di *Data Breach*

Nel caso in cui uno dei soggetti in precedenza indicati venga a conoscenza di una concreta, o solo potenziale o anche meramente sospetta violazione di dati personali, **dovrà attivare** il flusso di adempimenti più avanti descritti.
La gestione della violazione concreta, potenziale o sospetta prevede l'attuazione delle seguenti attività:
1. rilevazione e segnalazione della violazione dei dati personali,
2. raccolta delle informazioni sulla violazione e comunicazione della violazione,
3. valutazione del rischio,
4. individuazione delle possibili azioni correttive,
5. comunicazione delle valutazioni effettuate e delle azioni da intraprendere,
6. notifica della violazione (qualora necessaria),
7. documentazione delle violazioni (Registro dei *data breach*).

	Attivita	Interessati	Destinatari	Quando	Modalita'
1	**Rilevazione e segnalazione**	- personale dipendente - collaboratori - fornitori	- Responsabile della struttura - Responsabile per la sicurezza informatica - Responsabile per la transizione al digitale - RPD/DPO	Non appena ne viene a conoscenza	Modalità più veloci (telefono, email, ecc.)
2	**Raccolta delle informazioni**	Colui che ha rilevato la violazione	- Responsabile della struttura - Responsabile	Entro 24 ore	Modulo per la raccolta delle informazioni

			per la sicurezza informatica - Responsabile per la transizione al digitale - RPD/DPO		(allegato)
3	**Valutazione del rischio**	- RPD/DPO - Responsabile per la sicurezza informatica - Responsabile per la transizione al digitale		Non appena ne viene a conoscenza	Relazione cartacea
4	**Azioni correttive**	- RPD/DPO - Responsabile per la sicurezza informatica - Responsabile per la transizione al digitale		Dopo ogni revisione della DPIA	Integrazione della DPIA
5	**Comunicazione delle valutazioni e delle azioni**	- RPD/DPO - Responsabile per la sicurezza informatica - Responsabile per la transizione al digitale - Responsabili di struttura	Titolare		Relazione cartacea
6	**Notifica della violazione**	Titolare	Garante della privacy		Modello predisposto dal Garante
7	**Comunicazione agli interessati**	Titolare	Persone fisiche coinvolte		
8	**Documentazione**	- RPD/DPO - Responsabile per la sicurezza informatica		Non appena completate le sottostanti fasi	Inserimento dei dati nel Registro dei Data Breach

		- Responsabile per la transizione al digitale - Responsabili di struttura			

5. Violazione in caso di trattamenti di dati esternalizzati

Nel caso di trattamenti di dati esternalizzati, i Responsabili esterni del trattamento sono tenuti a comunicare al Titolare del trattamento (utilizzando l'allegato Modulo per la raccolta delle informazioni sulla violazione dei dati), per il tramite del Responsabile della Protezione dei Dati (RPD/DPO), l'avvenuta violazione **entro e non oltre 24 ore** dalla scoperta, al fine di consentire al Titolare di effettuare l'eventuale notifica al Garante e la comunicazione agli interessati entro i termini stabiliti dal Regolamento UE 679/2016.
Chiunque riceva segnalazioni di avvenute violazioni da parte di soggetti esterni, compresi i Responsabili esterni del trattamento, è tenuto a darne immediata comunicazione via mail al Responsabile della struttura di afferenza, al Responsabile per la Sicurezza informatica, al Responsabile della Transizione al digitale e al Responsabile per la Protezione dei Dati di Ateneo.
In tema il Garante, con Provvedimento del 30 luglio 2019 (Registro dei provvedimenti n. 157 del 30 luglio 2019) ha predisposto il modello di notifica delle violazioni dei dati personali (data breach), come riportato a pag. 7.

Allegato: Modulo per la raccolta di informazioni sulla violazione dei dati

Data della segnalazione:
Nome e cognome del segnalante:
Struttura di afferenza, funzione e dati di contatto del segnalante (tel., e-mail ecc.):
_____

1. Breve descrizione della violazione di dati personali

_____
_____
_____

2. Quando si è verificata la violazione di dati personali?

• Il _____
• Tra il _____ e il _____
• In un tempo non ancora determinato _____
• È possibile che sia ancora in corso _____

3. Luogo dove è avvenuta la violazione dei dati

(Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)
_____

4. Modalità di esposizione al rischio

_____

5. Tipologia di violazione

• Lettura (presumibilmente i dati non sono stati copiati)

_____

• Copia (i dati sono ancora presenti sui sistemi del Titolare) _____
• Alterazione (i dati sono presenti sui sistemi ma sono stati alterati) _____
• Cancellazione (i dati non sono più sui sistemi del Titolare e non li ha neppure l'autore della violazione) _____
• Furto (i dati non sono più sui sistemi del Titolare e li ha l'autore della violazione)

_____

• Altro _____

6. Dispositivo oggetto della violazione

• Computer
• Dispositivo mobile (specificare)
• Documento cartaceo (specificare)
• File o parte di un file
• Strumento di *backup*
• Rete
• Altro _____

7. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione

_____

_____

_____

_____

8. Persone che sono state colpite dalla violazione di dati personali

• N. ____
• Circa _____ persone
• Un numero (ancora) sconosciuto di persone

9. Tipologia di dati coinvolti nella violazione

• Dati anagrafici
• Numero di telefono (fisso o mobile)
• Indirizzo di posta elettronica
• Dati di accesso e di identificazione (user name, password, customer ID, altro)
• Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro) _____
• Altri dati personali (sesso, data di nascita, età, ...), dati sensibili e giudiziari
• Dato non ancora conosciuto

10. Livello di gravità della violazione dei dati personali

(secondo le valutazioni dell'Area/Struttura)

• Basso
• Medio
• Alto
• Molto alto

11. Misure tecniche e organizzative applicate ai dati colpiti dalla violazione

_____

_____

Metodologia di valutazione del rischio connesso alla violazione
Per identificare le modalità di gestione di una violazione e gli eventuali obblighi di notifica e/o di comunicazione, il Responsabile della Protezione dei Dati, con il supporto del Responsabile per la Sicurezza informatica e del Responsabile per la Transizione al digitale di Terre di Siena Lab nel caso di dati digitalizzati, effettua la
valutazione del rischio, come di seguito indicato.
Il livello di rischio è definito sulla base di due parametri: gravità e probabilità.

Gravità: rilevanza degli effetti dannosi che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte (es. impedendo il controllo da parte dell'interessato sulla diffusione dei propri dati).

Probabilità: grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).

Ai fini della identificazione dei valori da attribuire ai due parametri per la valutazione del rischio, sono considerati i seguenti fattori:
- tipo di violazione (violazione della riservatezza, violazione dell'integrità, violazione della disponibilità);
- natura, sensibilità e volume dei dati personali;
- facilità nella identificazione degli interessati;
- gravità delle conseguenze per gli interessati;
- particolarità degli interessati;
- particolarità dei responsabili del trattamento;
- numero degli interessati.

GRAVITA'
• Basso: nessun impatto
• Medio: impatto poco significativo, reversibile
• Alto: impatto significativo, irreversibile

PROBABILITA'
• Basso: l'evento temuto non si manifesta
• Medio: l'evento temuto potrebbe manifestarsi
• Alto: l'evento temuto si è manifestato

Rischio

DESCRIZIONE RISCHIO	NOTIFICA	COMUNICAZIONE
Basso: assenza di pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali utilizzati	**NO**	**NO**
Medio: possibile pregiudizio sui diritti e sulle libertà degli interessati e	**SI**	**NO**

sulla sicurezza dei dati personali utilizzati		
<u>Alto:</u> pregiudizio concreto e reale sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali utilizzati	**SI**	**SI**

Comunicazione della violazione all'interessato

Gentilissimo/a
_____

La informiamo che in data ..... siamo venuti a conoscenza di un evento che potrebbe aver coinvolto i suoi dati personali.

Presumiamo infatti che il _____, alle ore _____, un soggetto terzo non autorizzato abbia acquisito i seguenti dati personali relativi alla sua posizione:

- _____
- _____
- _____

Le possibili conseguenze dell'evento sono le seguenti:

Quale immediata reazione all'evento le confermiamo di aver adottato le seguenti misure di sicurezza:

Per maggiore garanzia e per ogni altra utilità, la invitiamo a:

Per qualsiasi informazione o chiarimento, potrà contattare il Responsabile della Protezione dei Dati (RPD/DPO) di Terre di Siena Lab,
_____,
ai seguenti recapiti:
- E-mail info@terredisienalab.it
- Pec: terredisienalab@pec.it