



Procedura di gestione della violazione dei dati personali

Data Breach Policy

Ordine delle Professioni Infermieristiche La Spezia

Versione 2.0 del 2 marzo 2025

Sommario

Sommario	1
1 - Introduzione	2
2 - Titolare del trattamento dati	2
3 - Responsabile della protezione dei dati	2
4 - Recapito per la segnalazione della violazione	2
5 - Procedura di gestione	3
5.1 - Rilevazione e segnalazione della violazione	4
5.2 - Raccolta informazioni e comunicazione della violazione	5
5.3 - Contenimento, recovery e risk assesment	6
5.4 - Notifica all'Autorità Garante (solo se necessaria)	7
5.5 - Comunicazione agli interessati coinvolti (solo se necessaria)	8
5.6 - Documentazione della violazione (Registro dei Data Breach)	9
Allegato A - Modulo per la raccolta informazioni	10

1 - Introduzione

Per violazione di dati personali deve intendersi ogni infrazione alla 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 dall'Ordine delle Professioni Infermieristiche della Spezia. (D'ora in poi: "dell'ente")

Lo scopo di questo documento è disegnare un flusso di procedure per la gestione delle anzidette violazioni.

Le procedure sono rivolte a tutti coloro che, nell'ente, trattano a qualsiasi titolo dati personali, quindi:

- i lavoratori dipendenti (al momento non presenti in OPI, che si avvale di iscritti eletti per la gestione delle attività d'istituto) ed i componenti il Consiglio Direttivo e della Commissione d'Albo che, a prescindere dal tipo di rapporto in essere, ha accesso ai dati personali trattati nel corso di prestazioni richieste per conto dell'ente;
- qualsiasi soggetto, persona fisica o persona giuridica, che, in ragione del rapporto contrattuale in essere con l'ente, abbia accesso ai dati e agisca in qualità di Responsabile del trattamento o di autonomo Titolare.

Il rispetto delle procedure è obbligatorio per tutti i soggetti coinvolti.

2 - Titolare del trattamento dati

Titolare del trattamento dati (o Titolare) è l'ORDINE DELLE PROFESSIONI INFERMIERISTICHE LA SPEZIA

3 - Responsabile della protezione dei dati

Il Responsabile per la Protezione dei Dati (o DPO) nominato dall'Ateneo, email: stefano.pileri@gmail.com

4 - Recapito per la segnalazione della violazione

Ogni violazione deve essere prontamente segnalata all'indirizzo segreteria@opi.laspezia.it con in oggetto: "violazione dati sensibili".

5 - Procedura di gestione

La gestione di una violazione dei dati personali prevede le seguenti fasi:

1. Rilevazione e segnalazione della violazione;
2. Raccolta informazioni e comunicazione della violazione;
3. Contenimento, recovery e risk assesment;
4. Notifica all'Autorità Garante (solo se necessaria);
5. Comunicazione agli interessati coinvolti (solo se necessaria);
6. Documentazione della violazione (Registro dei Data Breach). Le

single fasi sono meglio descritte nei seguenti paragrafi.

5.1 - Rilevazione e segnalazione della violazione

<i>Chi può segnalare</i>
Chiunque venga a conoscenza di una possibile violazione dei dati personali propri o altrui
<i>A chi segnalare</i>
Al Presidente pro tempore dell'ente
<i>Quando</i>
Appena se ne viene a conoscenza
<i>Come</i>
Utilizzando le vie più brevi (telefono, email, ecc.)

5.2 - Raccolta informazioni e comunicazione della violazione

<i>Chi deve raccogliere e comunicare</i>
Il Presidente dell'ente
<i>A chi inviare la comunicazione</i>
Al DPO e al referente del servizio informatico
<i>Quando</i>
Appena ricevuta la segnalazione
<i>Come</i>
Inoltrando il modulo di raccolta informazioni (Allegato A) debitamente compilato, tramite l'indirizzo email segreteria@opi.laspezia.it

5.3 - Contenimento, recovery e risk assesment

Chi agisce

Il DPO, d'intesa con il Presidente dell'ente e il referente del settore informatico

Destinatari

I soggetti incaricati di svolgere le attività di contenimento e recovery

Quando

Nei termini indicati nell'attività di risk assesment indicati dal DPO

Come

Valutazione dei rischi legati alla violazione accertata.

Valutazione della necessità di comunicazione della violazione al Garante e agli interessati e, in caso affermativo, informazione al Presidente affinché venga inoltrata la notifica al Garante.

Individuazione dei soggetti incaricati delle attività di contenimento e recovery.

Definizione delle operazioni da svolgere e dei tempi di attuazione

Comunicazione delle operazioni da effettuare ai soggetti incaricati

Eventuali operazioni di verifica di efficacia delle misure di contenimento e recovery stabilite ed eventuale prosecuzione delle indagini a seguito di indicazioni da parte del Garante, o del Presidente dell'ente come Titolare della sicurezza dei dati

5.4 - Notifica all'Autorità Garante (solo se necessaria)

<i>Chi la effettua</i>
Il Titolare dei dati (Presidente dell'ente), sentito il DPO
<i>A chi viene inoltrata</i>
Al Garante
<i>Quando</i>
Entro 72 ore dal momento in cui la violazione è rilevata
<i>Come</i>
Mediante la modulistica e i canali di comunicazione predisposti dal Garante

5.5 - Comunicazione agli interessati coinvolti (solo se necessaria)

<i>Chi la effettua</i>
Il Presidente, sentito il DPO
<i>A chi viene inoltrata</i>
Alle persone fisiche i cui dati sono stati violati
<i>Quando</i>
Nel più breve tempo possibile, senza ingiustificato ritardo
<i>Come</i>
Mediante comunicazione diretta o mediante pubblicazione in sito a loro accessibile

5.6 - Documentazione della violazione (Registro dei Data Breach)

<i>Chi compila il documento</i>
Il DPO insieme al Presidente dell'ente
<i>Quando</i>
Ogni volta che riceve la segnalazione di una violazione
<i>Come</i>
Registrazione della violazione nel Registro dei Data Breach con la descrizione della violazione, delle azioni intraprese e annotazione dei successivi aggiornamenti se necessario proseguire le indagini. Registrazione della risposta del Garante e delle eventuali prescrizioni in essa contenute. Registrazione della chiusura dell'incidente se non necessita di ulteriori indagini oppure indicazione della prosecuzione delle indagini.

Allegato A - Modulo per la raccolta informazioni

In caso di scoperta di un data breach:

1. Informare immediatamente il Presidente di OPI
2. Inviare a segreteria@opi.laspezia.it con oggetto: "violazione dati sensibili"

Data della violazione

- ☐ tra il __ / __ / ____ e il __ / __ / ____
- ☐ in un tempo non ancora determinato
- ☐ è possibile che sia ancora in corso

Luogo della violazione¹

Riferimenti di chi segnala la violazione²

Descrizione dell'evento in breve³

Banche dati oggetto di data breach e breve descrizione dei dati personali trattati

Tipo di violazione

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi)
- ☐ 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: _____

Tipo di dati oggetto della violazione

- ☐ Dati anagrafici
- ☐ Numero di telefono (fisso o mobile)
- ☐ Indirizzo di posta elettronica
- ☐ Dati di accesso e di identificazione (user name, password, altro)
- ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
- ☐ Altri dati di personali (sesso, data di nascita, età, ...), dati sensibili e giudiziari
- ☐ Altro: _____

Dispositivo oggetto della violazione

- ☐ Computer
- ☐ Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di backup
- ☐ Documento cartaceo
- ☐ Altro: _____

LE SEGNALAZIONI SARANNO CONSERVATE IN APPOSITO REGISTRO PROTETTO IN SEDE ENTE OPI LA SPEZIA

¹ Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili

² Indicare nome, cognome, email, telefono e altri dati di chi segnala

³ Riportare una descrizione sintetica del data breach, dei sistemi di elaborazione o memorizzazione dei dati coinvolti, la loro ubicazione, le categorie e il numero approssimativo di persone interessate dalla violazione