

**SEGNALAZIONE DI  
INCIDENTE DI SICUREZZA/VIOLAZIONE DI DATI PERSONALI**

*ai sensi dell'art. 33 del Regolamento Generale sulla Protezione dei Dati (RGPD)*

*Il presente modulo va compilato per la comunicazione al Titolare, RPD o CERT@unitn di un incidente di sicurezza che può comportare una violazione di dati personali, ai fini di una valutazione e gestione dell'incidente stesso e, in caso di violazione accertata, di eventuale notifica al Garante e di comunicazione agli interessati.*

*Le informazioni relative all'incidente devono essere raccolte prima possibile e il modulo compilato in ogni sua parte deve essere inviato al più presto all'indirizzo **rpm@unitn.it** e **cert@unitn.it** o trasmesso tramite il canale più breve disponibile al Titolare, RPD o CERT@unitn.*

*Il Titolare del trattamento è tenuto, 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 alla comunicazione agli interessati della violazione medesima.*

*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.*

*Laddove necessario alla prima valutazione possono seguirne altre, in base alle informazioni che vengono acquisite nella prosecuzione dell'indagine.*

**SEZ. A – DATI DEL SOGGETTO CHE EFFETTUA LA SEGNALAZIONE**

**A.1. Informazioni di contatto**

Dati identificativi del segnalante (nome e cognome): \_\_\_\_\_

Struttura di riferimento: \_\_\_\_\_

Telefono: \_\_\_\_\_ Email: \_\_\_\_\_

**SEZ. B – INFORMAZIONI DI SINTESI SULL'INCIDENTE/VIOLAZIONE**

**B.1. Informazioni sull'incidente**

Data e ora dell'incidente (anche approssimativi se non sono noti): \_\_\_\_\_

Data ed ora in cui il responsabile della struttura è venuto a conoscenza dell'incidente: \_\_\_\_\_

Luogo dell'incidente: \_\_\_\_\_

Modalità con la quale il responsabile della struttura è venuto a conoscenza dell'incidente:

---

---

**B.2. Breve descrizione dell'incidente:**

---

---

---

**B.3. Ambito del trattamento dei dati coinvolti:**

- Amministrazione
- Progetti di ricerca
- Didattica
- Altro (es. attività medico sanitaria): \_\_\_\_\_

**B.4. Tipo di incidente:**

- Riservatezza: Lettura (presumibilmente è stato effettuato un accesso ai dati ma i dati non sono stati copiati)
- Riservatezza: Copia (i dati sono ancora presenti sui sistemi del titolare ma copiati dall'autore della violazione)
- Integrità: Alterazione (i dati sono presenti sui sistemi del titolare ma sono stati alterati)
- Disponibilità: Cancellazione (i dati non sono più sui sistemi del titolare e non sono neppure in possesso dell'autore della violazione)
- Riservatezza e Disponibilità: Furto (i dati non sono più sui sistemi del titolare ma sono presumibilmente in possesso dell'autore della violazione)
- Disponibilità: Indisponibilità (i dati sono presenti sui sistemi del titolare ma non sono disponibili per un certo periodo di tempo)
- Altro: \_\_\_\_\_

**B.5. Causa dell'incidente:**

- Azione intenzionale interna
- Azione accidentale interna
- Azione intenzionale esterna
- Azione accidentale esterna



- Sconosciuta
- Altro: \_\_\_\_\_

**B.6. Categorie di dati personali oggetto dell'incidente:**

- Dati anagrafici/codice fiscale
- Dati di contatto (es: indirizzo email, numero di telefono)
- Dati di accesso e di identificazione (es. username, password, altro)
- Dati economico finanziari/pagamenti (es. numero carta di credito, numero di conto corrente)
- Dati relativi alla fornitura di servizi di comunicazione elettronica (es. log relativi al traffico internet)
- Dati giudiziari
- Dati di profilazione
- Dati relativi a documenti di identificazione (es. carta d'identità, passaporto, patente, CNS)
- Dati di localizzazione
- Dati personali idonei a rivelare l'origine razziale ed etnica
- Dati personali idonei a rivelare le opinioni politiche
- Dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere
- Dati personali idonei a rivelare l'adesione a partiti, sindacati
- Dati relativi alla vita sessuale e all'orientamento sessuale
- Dati genetici
- Dati relativi alla salute
- Dati biometrici
- Altro: \_\_\_\_\_

**B.7. Volume (anche approssimativo) dei dati personali coinvolti nell'incidente:**

- Indicare il volume di dati personali coinvolti: \_\_\_\_\_
- Indicare una stima dei dati personali coinvolti: \_\_\_\_\_



- Il volume dei dati personali non è noto

**B.8. Categorie di interessati coinvolti:**

- Personale docente e ricercatore
- Personale tecnico amministrativo
- Studenti
- Pazienti
- Minori
- Disabili
- Vulnerabili (es: vittime di violenza o abusi, rifugiati, richiedenti asilo)
- Altri Utenti: \_\_\_\_\_

**B.9. Numero (anche approssimativo) di interessati coinvolti nell'incidente:**

- Indicare il numero di interessati coinvolti: \_\_\_\_\_
- Indicare una stima del numero di interessati coinvolti: \_\_\_\_\_
- Il numero non è noto

**B.10 L'incidente coinvolge interessati di altri paesi:**

- Dello SEE<sup>1</sup> (indicare quali): \_\_\_\_\_
- Non appartenenti allo SEE (indicare quali): \_\_\_\_\_
- NO

**SEZ. C – INFORMAZIONI DI DETTAGLIO SULL'INCIDENTE/VIOLAZIONE**

**C.1 Descrizione dettagliata dell'incidente di sicurezza<sup>2</sup>:**

---

---

---

---

---

<sup>1</sup> Fanno parte dello Spazio Economico Europeo (SEE) tutti gli stati membri dell'Unione Europea, nonché l'Islanda, il Liechtenstein e la Norvegia

<sup>2</sup> Dettagliare quanto indicato nella sezione B ai punti 2, 3, 4, 5



---

## C.2 Descrizione delle categorie di dati personali oggetto dell'incidente<sup>3</sup>:

---

---

---

## C.3 Dispositivi oggetto dell'incidente:

- Computer/Laptop
- Server
- Storage
- Rete
- Dispositivo mobile (smartphone, tablet, ...)
- File o parte di un file
- Strumento di backup
- Documento cartaceo
- Altro: \_\_\_\_\_

## C.4 Ubicazione dei dispositivi oggetto dell'incidente:

---

---

## C.5 Descrizione delle misure di sicurezza tecniche ed organizzative, in essere al momento dell'incidente, adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolte:

---

---

---

---

<sup>3</sup> Dettagliare quanto indicato nella sezione B al punto 6



---

**SEZ. D – POSSIBILI CONSEGUENZE E GRAVITÀ DELL’INCIDENTE/VIOLAZIONE**

**D.1 Potenziali conseguenze dell’incidente sugli interessati<sup>4</sup>:**

**In caso di perdita di riservatezza:**

- I dati sono stati divulgati al di fuori di quanto previsto dall’informativa ovvero dalla disciplina di riferimento
- I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
- I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
- Altro: \_\_\_\_\_

**In caso di perdita di integrità:**

- I dati sono stati modificati e resi inconsistenti
- I dati sono stati modificati mantenendo la consistenza
- Altro: \_\_\_\_\_

**In caso di perdita di disponibilità:**

- Mancato accesso a servizi
- Malfunzionamento e difficoltà nell’utilizzo di servizi
- Altro: \_\_\_\_\_

**D.2 Ulteriori considerazioni sulle possibili conseguenze:**

---

---

---

**D.3 Descrizione dell’impatto dell’incidente/violazione sui diritti e le libertà degli interessati coinvolti:**

- Perdita del controllo dei dati personali
- Limitazione dei diritti
- Discriminazione
- Furto o usurpazione d’identità
- Frodi
- Perdite finanziarie

---

<sup>4</sup> Dettagliare in base a quanto indicato nella sezione B al punto 4



- 
- Decifratura non autorizzata della pseudonimizzazione
  - Pregiudizio alla reputazione
  - Perdita di riservatezza dei dati personali protetti da segreto professionale
  - Conoscenza da parte di terzi non autorizzati
  - Qualsiasi altro danno economico o sociale significativo:
- 

**SEZ. E – MISURE ADOTTATE A SEGUITO DELL’INCIDENTE/VIOLAZIONE**

**E.1 Misure tecniche e organizzative adottate (o di cui si propone l’adozione) per porre rimedio alla violazione e ridurre gli effetti negativi per gli interessati:**

---

---

---

**E.2 Misure tecniche e organizzative adottate (o di cui si propone l’adozione) per prevenire simili violazioni future:**

---

---

---

**SEZ. F – ULTERIORI INFORMAZIONI RELATIVE ALL’INCIDENTE/VIOLAZIONE**

**F.1 L’incidente è stato notificato ad altre autorità di controllo:**

- SI (indicare quali): \_\_\_\_\_
- NO

**F.2 L’incidente è stato segnalato all’autorità giudiziaria o di polizia:**

- SI
- NO

**F.3 Riportare di seguito ogni altra informazione ritenuta utile alla valutazione e gestione dell’incidente/violazione:**

---

---

---

---