UNIVERSITÀ DEGLI STUDI
DI TRENTO

MODULO DI COMUNICAZIONE DI UNA POTENZIALE VIOLAZIONE DI DATI PERSONALI

ai sensi dell'art. 33 del Regolamento Generale sulla Protezione dei Dati

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 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 ***rpd@unitn.it*** *e* ***cert@unitn.it*** *o trasmesso tramite il canale più breve disponibile al Titolare, RPD o CERT@unitn.*

Le Amministrazioni Pubbliche sono tenute, entro 72 ore dalla conoscenza di una violazione di dati personali, 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.

Informazioni di contatto

Dati identificativi del segnalante (nome e cognome): _____

Struttura di riferimento: _____

Telefono: _____ Email: _____

Informazioni sull'incidente di sicurezza

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

Luogo dell'dell'incidente: _____

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

Descrizione sintetica dell'incidente:

_____

_____

_____

Indicazione del/i trattamento/i inerente/i i dati personali coinvolti nell'incidente:

_____

_____

Finalità per le quale sono trattati i dati coinvolti:

- ☐ Amministrazione
- ☐ Progetti di ricerca
- ☐ Altro: _____ (es. attività medico sanitaria)

Tipo di violazione:

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

Dispositivo oggetto della violazione:

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

Descrizione sintetica dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

_____

_____

Volume dei dati personali coinvolti nella violazione:

- ☐ Indicare il volume, se noto, di dati personali coinvolti: _____
- ☐ Indicare una stima dei dati personali coinvolti: _____
- ☐ Il volume dei dati personali non è noto

Numero di persone fisiche interessate dalla violazione dei dati personali trattati:

- ☐ Indicare il numero, se noto, di persone fisiche coinvolte: _____
- ☐ Indicare una stima del numero di persone fisiche coinvolte: _____
- ☐ Il numero non è noto

Categorie di soggetti coinvolti:

- ☐ Personale docente e ricercatore
- ☐ Personale tecnico amministrativo
- ☐ Studenti
- ☐ Pazienti
- ☐ Minori
- ☐ Disabili
- ☐ Altri Utenti: _____

Categorie di dati personali oggetto della violazione:

- ☐ Dati anagrafici/codice fiscale
- ☐ Dati di accesso e di identificazione (es. username, password, altro)
- ☐ Dati relativi a minori
- ☐ Dati relativi a altri soggetti vulnerabili
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati
- ☐ Dati economico finanziari (es. numero carta di credito)
- ☐ Dati genetici
- ☐ Dati relativi alla salute

- ☐ Dati giudiziari
- ☐ Dati biometrici

Potenziali conseguenze della violazione:

_____

_____

_____

Descrizione dell'impatto della violazione sui diritti e le libertà degli interessati coinvolti:

_____

_____

_____

Descrizione di quali azioni siano state eventualmente già intraprese per fronteggiare gli eventuali effetti della violazione sui diritti e le libertà degli interessati coinvolti (es. aggiornamento delle password, azioni di formazione sulla sicurezza informatica):

_____

_____

_____