

MODULO DI SEGNALAZIONE DATA BREACH

(artt. 33 e 34 del Reg. UE 2016/679)

Designato al trattamento dati

Prof./Dott. _____

E-mail: _____

e p.c.

Responsabile per la protezione dei dati personali

Avv. Laura Mazzanti

e-mail: responsabileprotezionedati@unipi.it

Nome della persona che effettua la comunicazione: _____

Recapito telefonico: _____

e-mail: _____

Struttura (Direzione/Dipartimento/Sistema/Centro):

Breve descrizione dell'evento, con indicazione del luogo in cui è avvenuta la violazione:

Data dell'evento:

- Il _____
- Dal _____ (la violazione è ancora in corso)
- Dal _____ al _____
- In un tempo non ancora determinato
- In un tempo non determinabile

Causa della violazione:

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

Descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, e loro ubicazione:

Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti (es. in caso di furto di un pc presenza di bit locker, pc custodito in un cassetto chiuso a chiave etc.)

Categorie di interessati coinvolti nella violazione:

- Personale tecnico amministrativo
- Docenti
- Studenti
- Minori
- Pazienti
- Altro _____

Numero (anche approssimativo) di interessati coinvolti nella violazione:

- N. ___ interessati
- Circa N. ___ interessati
- Non determinabile
- Non ancora determinato

Categorie di dati personali oggetto di violazione (specificare, per ciascuna categoria di dati, quali sono i soggetti interessati dalla violazione):

- Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
- Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono)
- Dati di accesso e identificazione (username, password, ID, customer, altro)
- Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
- Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione Internet, altro)
- Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
- Dati di profilazione
- Dati relativi a documenti di identificazione/riconoscimento (carta d'identità, passaporto, patente, CNS, altro)
- Dati di localizzazione
- Dati che rilevino l'origine razziale o etnici
- Dati relativi a opinioni politiche
- Dati relativi a convinzioni religiose o filosofiche
- Dati che rilevino l'appartenenza sindacale
- Dati relativi alla vita sessuale o all'orientamento sessuale
- Dati relativi alla salute
- Dati genetici
- Dati biometrici
- Altro _____
- Categorie ancora non determinate

Numero (anche approssimativo) di registrazioni di dati personali oggetto di violazione:

- N. zero

- Circa N. __
- Non determinabile
- Non ancora determinato

Descrizione delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati:

Potenziale impatto della violazione:

- Perdita dei dati (i dati potrebbero comunque esistere, ma il Titolare ne ha perso il controllo o l'accesso, oppure non ne è più in possesso)
- Limitazione dei diritti
- Discriminazione
- Furto o usurpazione d'identità
- Frodi
- Perdite finanziarie
- Decifrazione non autorizzata della pseudonimizzazione
- Pregiudizio alla reputazione
- Perdita di riservatezza di dati personali protetti da segreto professionale
- Conoscenza da parte di terzi non autorizzati
- Altro _____

Dispositivo/i oggetto della violazione:

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

Gravità del potenziale impatto:

- Trascurabile
- Bassa
- Media
- Alta
- Non ancora definita

Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e ridurre gli effetti negativi:

Data

Firma