Modulo per la segnalazione di un potenziale *Data Breach* ai sensi del Regolamento dell'Unione Europea (UE) 2016/679 (GDPR)

Il presente modulo deve essere utilizzato per segnare un potenziale *Data Breach* relativo a dati personali afferenti banche dati di cui è titolare Università degli Studi di Milano.
Un *Data Breach* è una violazione di sicurezza che comporta 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.

Il modulo compilato in tutte le sue parti va inviato con la massima urgenza e senza ingiustificato ritardo, possibilmente entro 4-6 ore dall'accadimento e comunque non oltre le 24 ore - tramite email all'indirizzo: violazione.dati@unimi.it dalla casella di posta elettronica personale con indirizzo istituzionale @unimi.i**t.**

ATTENZIONE: quanto da voi comunicato verrà incorporato nella notifica che l'Università degli Studi di Milano farà all'Autorità Garante. Si ricorda quindi l'importanza di rendere dichiarazioni veritiere, onde evitare di incorrere nella sanzione penale prevista dall'art. 168 del D.Lgs. 196/03 in caso di false dichiarazioni all'Autorità Garante.

Versione 1.3 del 15 gennaio 2021

Dati di contatto di chi effettua la segnalazione *(* campi obbligatori):*

Nome e Cognome*:

Recapiti per comunicazioni dal DPO e/o dal team di gestione degli incidenti:

Indirizzo email*:

Telefono*:

Indirizzo (via / piazza, numero civico, Città e CAP)*:

Afferenza Organizzativa:

- Struttura/Ufficio di appartenenza*:
- Ruolo/Funzione ricoperta*:
- Nominativo del Responsabile della Struttura*:

Macro classificazione dell'incidente (può essere selezionata più di una voce):

☐ furto/smarrimento di device o supporto di memorizzazione (ad esempio: computer, smartphone, tablet, chiavetta USB, documenti cartacei, etc), indicare:

- quale device:
- si conosce il luogo in cui è avvenuto?
  - ☐ NO
  - ☐ SI, indicare il luogo:

☐ accesso abusivo a sistema informatico (ad esempio: Server, Data Base, Applicazione), specificare:

- denominazione del sistema:
- struttura che si occupa della gestione del sistema:
- collocazione fisica del sistema:
  - ☐ se interno all'Ateneo (locale, edificio, indirizzo):
  - ☐ se esterno all'Ateneo (nome del fornitore ed indirizzo):
- referente di un tecnico che si occupa della gestione del sistema:
  - ☐ nome e cognome:
  - ☐ recapito email:
  - ☐ recapito telefonico:

☐ Perdita/smarrimento/furto di credenziali di accesso a device (ad esempio: computer, smartphone, tablet, etc.) contenenti dati personali, indicare:

- nome account:
- consente accesso a:

☐ perdita/smarrimento/furto di credenziali di accesso ad applicazioni centrali (ad esempio: sistema documentale Archifflow, sistema gestione Carriera del Personale, sistema gestione Diritto allo Studio, sistema di rilevazione presenze, posta elettronica di Ateneo, etc.) contenenti dati personali, indicare:

- nome account:
- consente accesso a:

☐ perdita/smarrimento/furto di credenziali di accesso ad applicazioni dipartimentali contenenti dati personali indicare:

- nome account:
- consente accesso a:
- struttura che si occupa della gestione del sistema:
- referente di un tecnico che si occupa della gestione del sistema:
  - ☐ nome e cognome:
  - ☐ recapito email:
  - ☐ recapito telefonico:

Tipologia dei dati coinvolti (può essere selezionata più di una voce)**:**

☐ dati personali di dipendenti o collaboratori

☐ dati personali di familiari

☐ dati personali degli studenti

☐ dati personali di fornitori

☐ altri dati personali, specificare quali:

Dispositivo oggetto della violazione:

☐ computer

☐ rete

☐ dispositivo mobile

☐ file o parte di un file

☐ strumento di backup

☐ documento cartaceo

☐ altro, specificare:

Finalità per cui sono usati i dati coinvolti (compilare se sono note, può essere selezionata più di una voce)**:**

☐ processi amministrativi e gestionali dell'Ateneo

☐ progetti di ricerca

☐ attività didattica

☐ orientamento in ingresso o in uscita

☐ comunicazione e marketing

☐ altro, specificare:

Categorie dei dati coinvolti (può essere selezionata più di una voce)**:**

☐ dati anagrafici/codice fiscale/numero di matricola

☐ dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)

☐ dati di accesso e di identificazione (user name, password)

☐ dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)

☐ dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)

☐ 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, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale

☐ dati personali idonei a rivelare lo stato di salute, la vita sessuale e le preferenze sessuali

☐ dati relativi a minori

☐ dati giudiziari

☐ dati biometrici

☐ dati genetici

☐ ancora sconosciuto

☐ altro, specificare:

Tipo di violazione sui dati (può essere selezionata più di una voce)**:**

☐ lettura (presumibilmente i dati sono stati consultati ma non sono stati copiati)

☐ copia (i dati sono ancora presenti sul sistema/device ma sono anche stati copiati altrove)

☐ alterazione (i dati sono presenti sul sistema/device ma sono stati alterati)

☐ cancellazione (i dati non sono più presenti sul sistema/device e non li ha neppure l'autore della violazione)

☐ furto (i dati non sono più sul sistema/device e li ha l'autore della violazione)

☐ ancora sconosciuto

☐ altro, specificare:

Natura della violazione dei dati (può essere selezionata più di una voce)**:**

☐ distruzione o cancellazione non voluta di dati personali

☐ perdita di dati personali

☐ modifica non voluta di dati personali

☐ divulgazione non autorizzata o non voluta di dati personali

☐ accesso da parte di terzi ai dati personali trasmessi, conservati o comunque trattati

☐ non ancora noto

Numero di dati personali coinvolti (selezionare solo una voce):

☐ è noto il numero preciso di dati personali, indicare il numero:

☐ è nota una stima del numero di dati personali, indicare un valore stimato:

☐ non è noto il numero di dati personali.

Numero di interessati coinvolti (selezionare solo una voce):

☐ è noto il numero preciso di interessati, indicare il numero:

☐ è nota una stima del numero di interessati, indicare il numero:

☐ non è noto il numero di interessati.

Quando si è verificata la violazione dei dati personali? (selezionare solo una voce):

☐ è possibile identificare la data precisa della violazione e non è ancora in corso, il:

☐ è possibile identificare la data precisa di inizio della violazione ed è ancora in corso, il:

☐ è possibile identificare il seguente intervallo temporale nel quale è avvenuta la violazione, dal

al

Potenziali effetti negativi per gli interessati:

☐ perdita del controllo dei dati personali

☐ limitazione dei diritti

☐ discriminazione

☐ furto o usurpazione d'identità

☐ frodi

☐ perdite finanziarie

☐ 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 (specificare)

La violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo:

☐ Si (indicare quali): | |

☐ No

La violazione coinvolge interessati di Paesi non appartenenti dello Spazio Economico Europeo:

☐ Si (indicare quali): | |

☐ No

Eventuali ulteriori informazioni utili relative all'incidente:

Eventuali ulteriori informazioni utili relative ai sistemi su cui si è verificato l'incidente:

Note:

- Per la data del documento fa fede la data di invio della mail dalla casella di posta istituzionale;
- Si ricorda che chiunque dichiari o attesti falsamente notizie o circostanze o produca atti o documenti falsi verrà perseguito ai sensi di legge

firma

---

firma del Responsabile di Struttura
