**MODULO PER LA SEGNAZIONE DI UN POTENZIALE DATA BREACH**

**AI SENSI DEL REGOLAMENTO (UE) 2016/679**

Il presente modulo deve essere utilizzato per segnalare un potenziale data breach relativo a dati personali afferenti a banche dati di cui è titolare ERDIS Marche. Per data breach si intende «la 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» (art. 4 del Regolamento UE 2016/679).

**Il modulo compilato in tutte le sue parti va inviato tramite e-mail all’indirizzo:** [**direzione@erdis.it**](mailto:direzione@erdis.it)

**ATTENZIONE**: le informazioni fornite attraverso il presente modulo potrebbero essere inviate all’Autorità Garante al momento della notifica del data breach; per tale motivo, si ricorda 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 al Garante.

**DATI DI CONTATTO DI CHI EFFETTUA LA SEGNALAZIONE (\*campi obbligatori)**

Nome e cognome\*:

Recapiti per comunicazioni dal DPO e/o dal Team di risposta alle violazioni:

Indirizzo e-mail\* Telefono\*:

**AFFERENZA ORGANIZZATIVA**

Servizio/Ufficio di appartenenza\*:

Ruolo/Funzione ricoperta\*:

Nominativo del Responsabile della Struttura\*:

**MACROCLASSIFICAZIONE DELL’INCIDENTE** (può essere selezionata anche 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 e-mail:

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 gestione Diritto allo Studio, sistema di rilevazione presenze, posta elettronica istituzionale, 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 e-mail:

recapito telefonico:

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

**□** Dati personali di dipendenti o collaboratori

**□** 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

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

□ Processi amministrativi e gestionali dell’Ente

**□** Borse di studio e altri benefici a studenti

**□** Servizio ristorativo

**□** Servizio abitativo

**□** Appalti e contratti

**□** Concorsi e selezioni

**□** Altro, specificare:

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

□ dati anagrafici/codice fiscale/numero di matricola

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

□ 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

**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 ed 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

**Eventuali ulteriori informazioni utili relative all’incidente:**

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

Luogo e data

Firma del segnalante