

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

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

Nome e Cognome*:

Indirizzo e-mail* Telefono*:

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

Unità Organizzativa:

• Struttura/Ufficio di appartenenza*:

• Ruolo/Funzione ricoperta*:

• Nominativo del Responsabile di Area*:

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, sistema di rilevazione presenze, posta elettronica di Ateneo, ESSE3 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 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'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 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 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

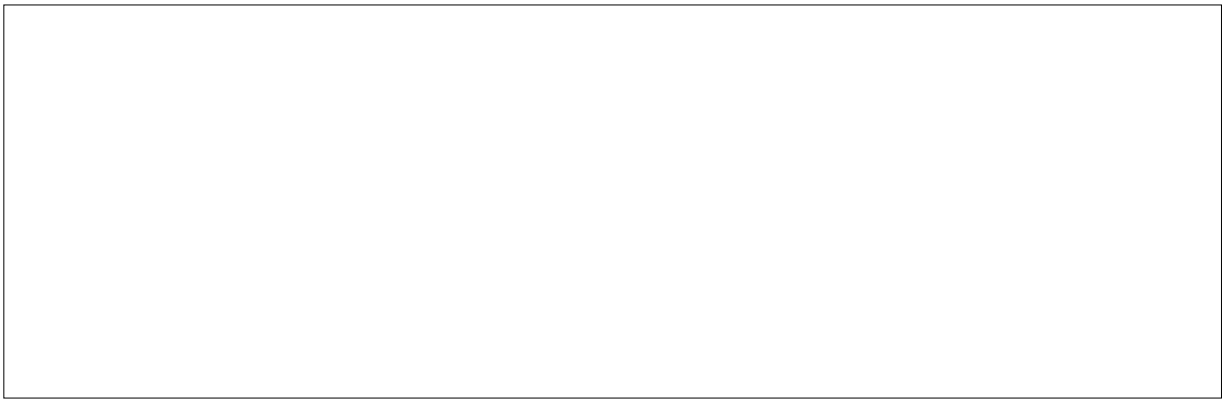
Numero di interessati coinvolti (selezionare solo una voce):

- è noto il numero preciso di interessati, indicare il numero:
- è 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 interessai

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

- E' possibile identificare la data precisa della violazione e non è ancora in corso, il:
- E' possibile identificare la data precisa di inizio della violazione ed è ancora in corso, il:
- E' 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:

