UNIVERSITÀ DI PARMA

MODULO PER LA SEGNAZIONE 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* realtivo a dati personali afferenti banche dati di cui è titolare l'Università.
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 tramite email all'indirizzo: databreach@unipr.it

UNIVERSITÀ DI PARMA

Dati di contatto di chi effettua la segnalazione:
(campi obbligatori)*
Nome e Cognome*:_____
Indirizzo email*: _____ @ _
Indirizzo email alternativo: _____ @ _
Telefono*: _____
Cellulare :_____
Indirizzo (nel caso di persona esterna all'Ateneo):
via*: _____ numero civico*___
Citta*: _____ CAP: _____

Afferenza Organizzativa: (nel caso di personale dell'Ateneo)
Struttura/Ufficio di appartenenza*: _____
Ruolo/Funzione ricoperta*:_____
Nominativo del Responsabile della Struttura*: _____

Quando è avvenuta o è venuto a conoscenza della violazione?
(gg/mm/aaaa) ___/___/_____ (hh:mm) _____:_____

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 congnome:_____
    - recapito email: _____
    - recapito telefonico:_____
- ☐ Perdita/smarrimaento/furto di credenziali di accesso a device o ad applicazione (ad esempio: computer, smartphone, tablet, etc.) contenenti dati personali, indicare:
  - nome account: _____
  - consente accesso a:_____
- ☐ Cancellazione/inaccessibilità di dati, specificare:
  - tipo di dispositivo: _____
- ☐ Altro: _____

Possibili cause della violazione delle proprie credenziali:

- ☐ Risposta ad un'email di phishing

- ☐ Possibile comunicazione o conoscenza delle credenziali da parte di persone note (p.e. collaboratori).
- ☐ Smarrimento di un supporto che le riportava scritte in chiaro o utilizzo da postazioni internet pubbliche
- ☐ Lettura da osservatore nelle vicinanze
- ☐ Coincidenza con password utilizzata per altri servizi on line, NON dell'Ateneo
- ☐ Altro:

_____
_____
_____
_____

Ha provveduto ad azioni per limitare i danni e se si, quali?

- ☐ Ho effettuato il cambio password
- ☐ Ho controllato tutti i miei dispositivi con un software antivirus e antimalware
- ☐ Altro:

_____
_____
_____
_____

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
- ☐ Dati personali di pazienti
- ☐ Altri dati personali, specificare quali:_____

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 e la vita sessuale
- ☐ 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: _____

Numero di dati (approssimativo) 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 interessai

È possibile che siano stati acceduti dati che possano comportare furto d'identità, perdite economiche, violazione di segreti d'ufficio o dati afferenti la salute (referti, diagnosi, …), la sfera sessuale o politica, fotografie, documenti contenenti dati potenzialmente pericolosi se utilizzati malevolmente? Se si, darne una descrizione:

_____
_____
_____

Eventuali ulteriori informazioni utili relative all'incidente:

_____
_____
_____
_____