

Modulo interno per la segnalazione di un potenziale *Data Breach*

Scopo del documento:	segnare un potenziale Data Breach relativo a dati personali trattati
Definizione di data breach:	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.
Tempistiche di invio del modulo:	massima urgenza e senza ingiustificato ritardo, possibilmente entro un'ora dall'accadimento, anche in orario extra lavorativo, tramite email all'indirizzo istituzionale

Dati di contatto di chi effettua la segnalazione:

Nome e Cognome:	
Ufficio/organo di appartenenza:	
Ruolo/Funzione ricoperta:	

Macro classificazione dell'incidente (barrare il quadratino corrispondente alla casella a sinistra e compilare la relativa casella di destra):

<input type="checkbox"/> Furto/Smarrimento di device o supporto di memorizzazione	Specificare tipologia di supporto (es computer, smartphone, tablet, chiavetta USB, documento cartacei.....) Specificare , ove si conosca il luogo
<input type="checkbox"/> Accesso abusivo a sistema informatico	Specificare denominazione del sistema (es: Server, Data Base, Applicazione....) Specificare struttura che si occupa della gestione del sistema Specificare collocazione fisica del sistema se interno all'istituto (locale, edificio, indirizzo) o se esterno (nome del fornitore e indirizzo del fornitore) Specificare referente di un tecnico che si occupa della gestione del sistema (nome e cognome, recapito email, recapito telefonico)
<input type="checkbox"/> Perdita/smarrimento/furto di credenziali di accesso a device (ad esempio:	indicare: -nome account: -consente accesso a:

computer, smartphone, tablet, etc.) contenenti dati personali	
<input type="checkbox"/> Perdita/smarrimento/furto di credenziali di accesso piattaforme contenenti dati personali	indicare: -nome account: -consente accesso a:

Tipologia dei dati coinvolti:

<input type="checkbox"/> Dati personali di dipendenti o collaboratori
<input type="checkbox"/> Dati personali dei clienti
<input type="checkbox"/> Dati personali di fornitori
<input type="checkbox"/> Altri dati personali, specificare quali:

Dispositivo oggetto della violazione:

<input type="checkbox"/> Computer
<input type="checkbox"/> portatile
<input type="checkbox"/> Strumento di backup (es. hw esterno)
<input type="checkbox"/> Documento cartaceo
<input type="checkbox"/> Dispositivo mobile (es. tablet, smartphone, chiavetta usb, ecc..)
<input type="checkbox"/> Altro

Finalità per cui sono usati i dati coinvolti

<input type="checkbox"/> Gestione utenti
<input type="checkbox"/> Gestione rapporto di lavoro
<input type="checkbox"/> Gestione fornitori
<input type="checkbox"/> Altro

Categorie dei dati coinvolti

<input type="checkbox"/> dati anagrafici/codice fiscale/numero di matricola
<input type="checkbox"/> dati di accesso e di identificazione (user name, password)
<input type="checkbox"/> 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
<input type="checkbox"/> dati personali idonei a rivelare lo stato di salute
<input type="checkbox"/> dati giudiziari
<input type="checkbox"/> dati biometrici
<input type="checkbox"/> altro, specificare:

Tipo di violazione sui dati:

<input type="checkbox"/> lettura (presumibilmente i dati sono stati consultati ma non sono stati copiati)
<input type="checkbox"/> copia (i dati sono ancora presenti sul sistema/device ma sono anche stati copiati altrove)
<input type="checkbox"/> alterazione (i dati sono presenti sul sistema/device ma sono stati alterati)
<input type="checkbox"/> cancellazione (i dati non sono più presenti sul sistema/device/ e non li ha neppure l'autore della violazione)
<input type="checkbox"/> esfiltrazione - furto (i dati non sono più sul sistema/device e li ha l'autore della violazione)
<input type="checkbox"/> ancora sconosciuto
<input type="checkbox"/> altro, specificare:

Natura della violazione dei dati

<input type="checkbox"/> distruzione o cancellazione dolosa di dati personali
<input type="checkbox"/> perdita di dati personali involontaria
<input type="checkbox"/> modifica non voluta di dati personali
<input type="checkbox"/> divulgazione non autorizzata o non voluta di dati personali
<input type="checkbox"/> accesso da parte di terzi ai dati personali trasmessi, conservati o comunque trattati

--

Numero di dati personali coinvolti

<input type="checkbox"/> è noto il numero preciso di dati personali	indicare il numero:
<input type="checkbox"/> è nota una stima del numero di dati personali	indicare un valore stimato
<input type="checkbox"/> non è noto il numero di dati personali	

Numero di interessati coinvolti

<input type="checkbox"/> è noto il numero preciso di interessati	indicare il numero:
<input type="checkbox"/> è nota una stima del numero di interessati	indicare il numero:
<input type="checkbox"/> non è noto il numero di interessati	

Quando si è verificata la violazione dei dati personali?

<input type="checkbox"/> E' possibile identificare la data precisa della violazione
<input type="checkbox"/> E' possibile identificare la data precisa di inizio della violazione ed è ancora in corso
<input type="checkbox"/> E' possibile identificare il seguente intervallo temporale nel quale è avvenuta la violazione, dal _____ al _____

Eventuali ulteriori informazioni utili relative all'incidente:

Terni, lì

Firma
