**MODULO PER LA SEGNALAZIONE DI VIOLAZIONI DEI DATI PERSONALI**

**Obbligatoria ai sensi degli artt. 33 e 34 R. UE. 679/2016**

**Attenzione**: valutare, per il tipo di violazione riscontrata, se cambiare immediatamente la password utilizzataper la posta istituzionale d’Ateneo o i servizi d’ateneo, eventualmente procedendo immediatamente a cambiarla anche per i servizi, diversi da quelli dell’Ateneo, nei quali utilizza la stessa password.

Le informazioni che fornirà per la segnalazione sono necessari alla stima del problema e alla sua gestione ai sensi del R.UE. 679/2016, artt.33 e 34: **dovranno pertanto essere il più possibile complete ed esatte** al fine di garantire il rispetto dei tempi previsti dal Regolamento UE per la comunicazione al Garante entro le 72h, qualora dalla stima risultasse necessario procedere in tal senso.

Per lo stesso motivo il presente modulo deve essere trasmesso all’indirizzo databreach@unistrapg.it il più tempestivamente possibile, anche da e-mail privata.

I dati personali che comunicherà saranno utilizzati solo a tale scopo come da **INFORMATIVA.**

**Dati di contatto per eventuali ulteriori informazioni o approfondimenti:**

nome e cognome:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

cellulare: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Quando è avvenuta la violazione?**

(gg/mm/aaaa) \_\_\_/\_\_\_/\_\_\_\_\_\_\_ (hh:mm) \_\_\_\_\_:\_\_\_\_\_

1. **Tipologia di violazione**
* Furto, perdita o smarrimento di dispositivi elettronici contenenti dati
* Violazione del sistema informatico o supporto informatico (anche tentativi importanti non andati a buon fine)
* Diffusione non autorizzata dei dati
* Accesso a banche dati da utenti non autorizzati
* Altro: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
1. **Quando è stata scoperta la violazione?**

(gg/mm/aaaa) \_\_\_/\_\_\_/\_\_\_\_\_\_\_ (hh:mm) \_\_\_\_\_:\_\_\_\_\_

1. **Luogo dove si è verificata la violazione o dove risiedono i siti violati:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Dispositivo o sistema oggetto della violazione:**
* Sistema centrale
* Sistema centrale di rete
* Server dipartimentale/centro
* Postazione di lavoro (Computer fisso)
* Dispositivo mobile (pc, smartphone, hard disk, chiave usb,….)
* Supporto cartaceo
1. **Categorie di dati che sono stati violati:**
* dati anagrafici, codice fiscale, matricole (con dati di contatto o residenza ? \_\_\_\_\_ )
* dati di identificazione ai servizi (userid/password, posta elettronica,..)
* dati di accesso ai gestionali dell’ateneo
* dati di natura particolare (origine razziale o etnica, orientamento religioso, politico, sindacale, salute, handicap, vita sessuale, immagini,..)
* dati personali registrati in database di ateneo
* altro:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Descrizione della natura della violazione dei dati personali:**
* Visualizzazione: lettura da un numero esiguo di destinatari, senza possibilità di copia
* Comunicazione: resi noti a destinatari non autorizzati e identificabili
* Diffusione: esposizione per errore a destinatari numericamente non conoscibili
* Copia: è stata possibile una duplicazione illecita con i dati inalterati su dispositivi ancora disponibili
* Alterazione: i dati sui sistemi hanno subìto delle manipolazioni non autorizzate
* Cancellazione: i dati non sono più disponibili sui sistemi del titolare e neppure altrove
* Perdita: i dati esistono ancora, ma senza possibilità di controllo o di accesso
* Furto: i dati non sono più disponibili sui sistemi del titolare ma sono in possesso di un Terzo
* Altro: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
1. **Categorie di interessati cui afferiscono i dati oggetto della violazione:**
* Studenti
* Personale
* Collaboratori
* Fornitori
* Forniti da Enti esterni, altri organismi
* Altro:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
1. **numero (anche approssimativo) di persone coinvolte dalla violazione:**
* numero \_\_\_\_\_
* circa \_\_\_\_\_\_\_
* al momento non stimabile
1. **numero di registrazioni interessate, in caso di database:**
* numero stimabile di occorrenze: \_\_\_\_\_\_\_\_\_\_
* occupazione in GB: \_\_\_\_\_\_\_\_\_\_\_\_

1. **probabili conseguenze per gli interessati per la tipologia di dati personali violati:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. **Ha provveduto ad azioni per limitare i danni e se si, quali?**
* Ho effettuato il cambio password
* Ho bloccato il dispositivo nelle successive \_\_\_ ore
* Ho aggiornato i dispositivi con un software antivirus e antimalware
* Ho disponibili copie di backup dei dati
* Avevo crittografato i dati
* Avevo protetto l’accesso al dispositivo/dati con password
* Altro: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
1. **E’ 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**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Inoltrarlo via email a databreach@unistrapg.it

**Grazie della collaborazione!**