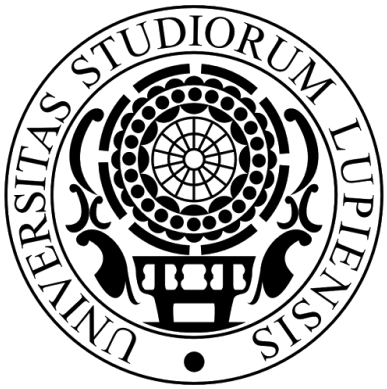
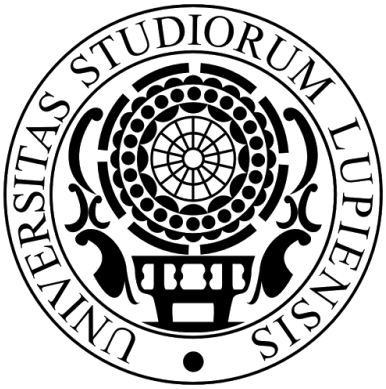


UNIVERSITÀ
DEL SALENTO

Procedura di DataBreach
Università del Salento

Indice



UNIVERSITÀ
DEL SALENTO

Procedura di DataBreach dell'Università del Salento

Riferimenti normativi	Artt. 33 e 34 del Regolamento Generale sulla Protezione dei Dati (UE/2016/679)
Titolare del trattamento	Magnifico Rettore dell'Università del Salento Sito web: https://www.unisalento.it
DPO (Data Protection Officer)	Dott.ssa Giusy Campanile Email: dpo@unisalento.it Telefono: 0832292333 Pagina web: https://www.unisalento.it/people/giusy.campanile

Step 1	
Attività	**Segnalazione del sospetto DataBreach**
Attore	Segnalante: Dipendente, fornitore, collaboratore.
Quando	Non appena si ha contezza del possibile DataBreach
Come	Inviando un'email a databreach@unisalento.it
Descrizione	Non appena si sospetti un DataBreach il segnalante deve inviare la segnalazione a mezzo email descrivendo l'evento occorso includendo l'apposito modulo di segnalazione.

Step 2	
Attività	**Presa in carico e prima analisi**
Attore	DPO
Quando	Non appena si riceve una segnalazione
Come	Tramite il modello allegato

Descrizione	Il DPO effettua una prima analisi della segnalazione per conferma o meno di DataBreach. Eventuali prime azioni di rimedio dell'incidente assieme al referente IT dell'applicazione se relativa ai sistemi interni.

Step 3.1	
Attività	**Notifica al Titolare sospetto DataBreach**
Attore	DPO
Quando	Dopo lo step 2 se si sospetta un DataBreach
Come	Tramite le vie più brevi
Descrizione	Il DPO Notifica Rettore, Direttore Generale, Dirigente RTT, e Responsabile della Struttura titolare dell'applicativo (o Responsabile del Centro / Dipartimento in cui il DataBreach è avvenuto) oggetto del DataBreach riportato nel registro dei trattamenti.

Step 3.2	
Attività	**Notifica al Segnalante assenza DataBreach**
Attore	DPO
Quando	Dopo lo step 2 se non si sospetta un DataBreach
Come	Tramite le vie più brevi
Descrizione	Il DPO Notifica il segnalante circa l'insussistenza del DataBreach ed esegue lo step 10.

Step 4	
Attività	**Analisi del DataBreach**
Attore	Responsabile IT dell'Applicazione (o Fornitore Esterno)
Quando	Dopo lo step 3.1
Come	

Descrizione	In caso di sospetto DataBreach il DPO allerta il Responsabile IT dell'applicazione (o il fornitore esterno) e assieme ad esso e al Responsabile di Struttura Titolare dell'applicativo effettua una analisi dettagliata del DataBreach

Step 5.1	
Attività	**Predisposizione relazione analisi**
Attore	Responsabile IT dell'Applicazione (o Fornitore Esterno)
Quando	Se lo step 4 ha confermato il DataBreach
Come	A mezzo email o protocollo
Descrizione	In caso di DataBreach confermato allo step 4 si predispone ed invia una relazione dettagliata (predisposta assieme al DPO e al Responsabile di Struttura titolare dell'applicativo coinvolto nella violazione) al Titolare del Trattamento. La relazione contiene eventuali elementi per ripristinare il servizio (modalità, tempistiche ecc...)

Step 5.2	
Attività	**Mancata conferma del DataBreach**
Attore	DPO
Quando	Se lo step 4 NON ha confermato il DataBreach
Come	A mezzo email o protocollo
Descrizione	In caso di DataBreach non confermato allo step 4 il DPO ne da' Notifica al Rettore, al Direttore Generale, al Dirigente RTT e al Responsabile di Struttura titolare dell'applicativo oggetto del DataBreach. Esegue quindi lo step 10.

Step 6	
Attività	**Analisi delle azioni da intraprendere**
Attore	Titolare

Quando	Dopo lo step 5.1
Come	Analizzando la relazione prodotta
Descrizione	Il Titolare analizza la relazione prodotta e fornisce indicazioni su come procedere e su quali azioni intraprendere.

Step 7	
Attività	**Valutazione dell'impatto del DataBreach**
Attore	Titolare
Quando	Dopo lo step 6
Come	
Descrizione	Il Titolare, se necessario, notifica al Garante la violazione rilevata utilizzando la modulistica predisposta sul sito del Garante

Step 8.1	
Attività	**Notifica al Garante (eventuale)**
Attore	Titolare
Quando	Dopo lo step 7 ed **entro 72 ore dalla Rilevazione**
Come	
Descrizione	Il Titolare, se necessario, notifica al Garante la violazione rilevata utilizzando la modulistica predisposta sul sito del Garante

Step 8.2	
Attività	**Notifica agli interessati (eventuale)**
Attore	Titolare
Quando	Dopo lo step 7
Come	

Descrizione	Il Titolare, se necessario, notifica agli interessati la violazione rilevata

Step 9	
Attività	**Mitigazione del DataBreach**
Attore	Responsabile IT dell'Applicazione (o Fornitore Esterno)
Quando	Dopo lo step 6
Come	
Descrizione	Vengono attuate la azioni necessarie volte a mitigare, attenuare o risolvere la violazione riscontrata.

Step 10	
Attività	**Aggiornamento Registro delle Violazioni**
Attore	DPO
Quando	Dopo lo step 6 o dopo lo step 3.2
Come	
Descrizione	Il DPO aggiorna il registro delle violazioni in base a quanto evidenziato dall'analisi includendo le notifiche inviate e le azioni correttive svolte.

La procedura è descritta nell'allegato **all1_procedura_data_breach.pdf**

Descrizione dei soggetti richiamati nella procedura

Segnalante – è colui che ha segnalato il sospetto DataBreach.

Titolare - è il titolare del trattamento dei dati personali, cioè il Magnifico Rettore dell'Università del Salento

DPO - è il Responsabile della protezione dati dell'Ateneo; l'incarico è stato assegnato alla Dott.ssa Giusy Campanile

Responsabile della struttura – a seconda della struttura può essere il dirigente, il direttore tecnico, il presidente, il direttore, il responsabile amministrativo. In sua assenza segue la procedura il sostituto o il referente privacy.

Responsabile IT dell'Applicazione – è colui che materialmente gestisce l'applicazione o il sistema oggetto del DataBreach: può essere sia un tecnico dell'amministrazione centrale, che un tecnico di un centro / Dipartimento, che un fornitore esterno.

Garante – è l'autorità garante in Italia (http://www.garanteprivacy.it/) alla quale i titolari si rivolgono per gli adempimenti previsti dal GDPR (Regolamento UE 2016/679 del Parlamento Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Interessato – è la persona fisica alla quale si riferiscono i dati personali. Gli interessati possono essere raggruppati in categorie, quali ad esempio studenti, personale dipendente, collaboratori, ecc.

FAQ

Cosa è un DataBreach?

E' una violazione di sicurezza che comporta accidentalmente o in modo illecito:

- la distruzione,
- la perdita,
- la modifica,
- la divulgazione non autorizzata
- l'accesso

ai dati personali trasmessi, conservati o comunque trattati.

Cosa si intende per *distruzione* di dati?

L'evento in base al quale i dati non esistono più o comunque non sono più nelle condizioni di essere utilizzati dal Titolare.

Cosa si intende per *modifica* di un dato?

L'alterazione di un dato, la corruzione di un dato, l'incompletezza del dato.

Cosa si intende per *perdita* di un dato?

La condizione in cui il Titolare non può più controllare o disporre dei dati.

Cosa si intende per *divulgazione* di un dato?

La diffusione di dati; la condivisione dei dati con soggetti non autorizzati.

Cosa fare se…

Ho smarrito una cartella contenente, tra le altre cose, l'elenco degli ammessi alle prossime sedute di laurea con relativi dati personali degli studenti. Devo fare segnalazione?

Sì, è necessario inoltrare la segnalazione.

Ho smarrito lo smartphone su cui erano memorizzati messaggi di posta elettronica della mia casella UNISALENTO, devo effettuare la segnalazione?

La segnalazione è necessaria se esiste il dubbio che eventuali dati personali contenuti nei messaggi di posta possano essere acceduti da terzi o se sono andati perduti. Non è necessaria se esiste una copia dei dati e se siamo certi che lo smartphone non può essere utilizzato da altri.

Il computer dell'ufficio è stato formattato in seguito ad un guasto. Devo fare la segnalazione?

Se esiste un backup dei dati personali contenuti nel computer, non è necessaria la segnalazione.

Ho trovato che è stata forzata la serratura di un armadio contenente archivi cartacei relativi alle carriere del personale tecnico amministrativo, ma sembra che non manchi nulla. Devo fare la segnalazione?

Sì, è necessario inoltrare la segnalazione.

È stato rubato un laptop da un ufficio, nel quale erano contenuti dati personali di studenti. Devo fare la segnalazione?

Sì, è necessario inoltrare la segnalazione.

Per errore ho inviato un messaggio di posta elettronica contenente una lista di studenti iscritti ad un corso con indicazione di matricola ed indirizzo e-mail a più destinatari sbagliati. Devo fare la segnalazione?

Sì, è necessario inoltrare la segnalazione.

Ho lasciato, per sbaglio, alcune domande per usufruire della 104 su un bancone dell'ufficio a cui accedono più persone anche esterne. Devo fare la segnalazione?

Sì, è necessario inoltrare la segnalazione.

Non so chi devo informare di una violazione di dati personali che ho trovato su una pagina del sito web di Ateneo.

La segnalazione deve essere effettuata al responsabile della propria struttura di afferenza, il quale avvierà la procedura per la comunicazione al Titolare. In mancanza di questi contattare direttamente il Responsabile della protezione dati (DPO) di Ateneo o il suo ufficio.

Mi sono accorto che un vecchio computer è stato hackerato. Apparentemente non sono stati rubati dati. Devo fare la segnalazione?

È necessario effettuare la segnalazione.

Allegato n1: Procedura di DataBreach