Procedura segnalazione VIOLAZIONE DATI PERSONALI (*DATA BREACH*)

Titolare del trattamento dati: Università degli Studi di Firenze

Responsabile della Protezione dei dati (RPD): dott. Massimo Benedetti – privacy@unifi.it – tel.: +39 055 2757667

Attività di segnalazione, raccolta informazioni, valutazione notifica della violazione

STEP	ATTIVITA'	CHI	A CHI	QUANDO	COME
1	**Rilevazione e segnalazione di data breach**	Tutto il personale, collaboratori, fornitori, responsabili	Al Responsabile amministrativo della struttura di riferimento (Dirigente, RAD, Direttore Tecnico) o al suo sostituto o al referente privacy se nominato	Appena se ne viene a conoscenza	Utilizzando le vie più brevi (telefono, di persona, e-mail)
2	**Raccolta informazioni sulla violazione**	Il responsabile della struttura o il sostituto o il referente privacy insieme ai soggetti coinvolti nella violazione (il responsabile della struttura nel caso non possa essere immediatamente disponibile, deve dare		Appena ricevuta la comunicazione	Utilizzando il modello fornito e raccogliendo informazioni dai soggetti coinvolti nella segnalazione e nel trattamento dei dati violati

		istruzioni precise alla persona che l'ha contattato per iniziare subito la raccolta delle informazioni, indicando dove reperire il modello predisposto a tale scopo)			
3	**Comunicazione del data breach**	Il responsabile amministrativo della struttura (RAD, Direttore Tecnico, Dirigente) o il sostituto o il referente privacy (in mancanza di tali figure la stessa persona che ha rilevato la violazione)	Al Titolare (da specificare quale organo di UNIFI è incaricato della notifica della violazione al Garante), RPD, esperti ICT	Appena ottenute informazioni di base sulla violazione	Utilizzando le vie più brevi
4	**Valutazione d'impatto**	Titolare, RPD, esperti ICT, soggetti coinvolti		Appena ricevuta la comunicazione	Utilizzando la metodologia indicata
5	**Individuazione delle azioni correttive**	RPD, esperti ICT, soggetti coinvolti		Appena terminata la valutazione d'impatto	Analizzando i risultati della valutazione d'impatto
6	**Comunicazione delle valutazioni effettuate e delle azioni da intraprendere**	RPD, responsabile della struttura o sostituto o referente privacy	Al Titolare		Tramite una breve relazione anche orale
7	**Notifica della violazione (se è necessaria)**	Titolare	Al Garante	Entro 72 ore dalla rilevazione	Mediante la modulistica predisposta dal Garante
8	**Comunicazione agli interessati coinvolti (se è necessaria)**	Titolare	Alle persone fisiche i cui dati sono stati violati	Nei termini indicati nella valutazione d'impatto	Comunicazione diretta alle singole persone o mediante pubblicazione in sito a loro accessibile delle eventuali conseguenze della violazione sulle categorie di persone fisiche interessate

9	**Disposizioni per l'attuazione delle misure correttive (se individuate)**	Responsabili delle strutture coinvolte	Ai soggetti incaricati di svolgere le attività	Nei termini indicati nella valutazione d'impatto	Devono essere indicate in dettaglio le operazioni da svolgere, chi è l'incaricato, i tempi di attuazione; prevedere eventuali operazioni di verifica dell'efficacia delle misure correttive
10	**Recepimento della risposta del Garante alla notifica (se effettuata)**	Titolare, RPD, responsabili delle strutture coinvolte, esperti ICT			Disposizioni per l'attuazione delle eventuali misure correttive indicate dal Garante; effettuazione di ulteriori indagini per approfondire le informazioni raccolte

Attività relative alla registrazione dell'incidente

STEP	ATTIVITA'	CHI	A CHI	QUANDO	COME
1	**Registrazione della violazione/aggiornamenti**	Ufficio RPD		Appena ricevuta la comunicazione	Compilando l'apposito registro con la descrizione della violazione, delle azioni intraprese e annotando i successivi aggiornamenti
2	**Registrazione della risposta del Garante**	Ufficio RPD		Al momento della ricezione	Annotando sul registro gli estremi della risposta del Garante e le eventuali prescrizioni in essa contenute
3	**Registrazione della prosecuzione/chiusura dell'incidente**	Ufficio RPD		In seguito alle indicazioni del RPD	Registra la chiusura dell'incidente se non necessita di ulteriori indagini o riporta le istruzioni per le ulteriori indagini

Attività inerenti la prosecuzione delle indagini

Da eseguire nel caso sia necessario acquisire ulteriori informazioni

STEP	ATTIVITA'	CHI	A CHI	QUANDO	COME
1	**Prosecuzione delle indagini**	RPD, responsabile della struttura o sostituto o referente privacy, soggetti coinvolti nella violazione e nei trattamenti di dati violati, esperti ICT		A seguito di indicazione da parte del Garante o del titolare; se previsto nella prima valutazione d'impatto; nel caso che le informazioni raccolte risultino incomplete o mancanti	Raccogliendo le informazioni mancanti, o approfondendo quelle note per rilevare eventuali impatti non riscontrati nella prima indagine
2	**Esecuzione di una nuova valutazione d'impatto**	Titolare, RPD, esperti ICT, soggetti coinvolti		Al momento che si ritiene di aver raccolto tutte le informazioni possibili sulla violazione	
3	**Comunicazione dei risultati del proseguimento delle indagini**	RPD, responsabile della struttura o sostituto o referente privacy	Al Titolare	appena terminato il lavoro	Tramite relazione sintetica sui risultati della valutazione d'impatto e sulle azioni necessarie, allegando il materiale informativo raccolto
4	**Aggiornamento della notifica al Garante (se necessario)**	Titolare	Al Garante	Appena sono disponibili i nuovi dati o secondo i termini stabiliti dal Garante	Mediante la modulistica predisposta o come indicato dal Garante
5	**Comunicazioni agli interessati (se necessario)**	Titolare		Nei tempi stabiliti nella valutazione	Contattando direttamente gli interessati oppure rendendo nota la violazione e le

				d'impatto	possibili conseguenze mediante pubblicazione accessibile alle categorie di interessati

Descrizione dei soggetti richiamati nelle procedure

Titolare - è il titolare del trattamento dei dati personali, cioè l'Università degli Studi di Firenze

RPD – è il Responsabile della protezione dati dell'Ateneo (detto anche DPO - Data Protection Officer). L'incarico è stato assegnato al dott. Massimo Benedetti

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

Referente privacy – è colui che ha avuto specifico incarico per gestire gli adempimenti in materia di protezione dei dati personali all'interno della propria struttura.

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.

Ufficio RPD – Ufficio Funzionale di supporto al Responsabile della Protezione dei dati (https://www.unifi.it/cercachi-str-101495.html)

FORM PER RACCOLTA INFORMAZIONI

1. luogo e data dell'evento (anche approssimativi se non sono noti): _____
2. breve descrizione dell'evento:

   _____
3. indicazione dei trattamenti di dati coinvolti *(riportare elenco dei trattamenti?)*

   _____
4. banche dati o archivi anche cartacei che sono stati violati:

   _____
5. tipo di violazione
   - ☐ lettura (presumibilmente i dati non sono stati copiati)
   - ☐ copia (i dati sono ancora presenti sul sistema del titolare)
   - ☐ alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
   - ☐ cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
   - ☐ furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
   - ☐ altro: _____
6. Dispositivo oggetto della violazione
   - ☐ Computer
   - ☐ Rete
   - ☐ Dispositivo mobile
   - ☐ File o parte di un file
   - ☐ Strumento di backup
   - ☐ Documento cartaceo
   - ☐ Altro: _____

7. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione: _____
8. Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?
   - ☐ N. _____persone
   - ☐ Circa _____persone
   - ☐ Un numero (ancora) sconosciuto di persone
9. Che tipo di dati sono oggetto di violazione?
   - ☐ Dati anagrafici/codice fiscale
   - ☐ Dati di accesso e di identificazione (user name,password, customer ID, altro)
   - ☐ Dati relativi a minori
   - ☐ 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

INFORMAZIONI PER LA COMPILAZIONE

DEFINIZIONI

<violazione di dati personali (data breach)>

la violazione di sicurezza che comporta accidentalmente o in modo illecito:

- la distruzione,
- la perdita,
- la modifica,
- la divulgazione o l'accesso non autorizzati

ai dati personali trasmessi, conservati o comunque trattati.

<distruzione (destruction)>

Non esistono più i dati

Non esistono più in forma che possa essere utilizzata dal titolare

<modifica (alteration, damage)>

Alterazione del dato

Corruzione del dato

Incompletezza del dato

<Perdita (loss)>

Il titolare non ha più il controllo sui dati

Il titolare non ha più i dati

<divulgazione (unauthorized or unlawful processing)>

Divulgazione di dati

Accesso ai dati da parte di destinatari non autorizzati

Trattamenti in violazione del GDPR

Elenco principali trattamenti di dati personali svolti in Ateneo

Trattamenti inerenti gli studenti :

- finalizzato all'orientamento
- finalizzato all'erogazione dei test di ingresso o alla verifica dei requisiti di accesso
- finalizzato per il percorso formativo e gestione della carriera
- finalizzato all'attività di tirocinio
- finalizzato all'attività di job placement
- finalizzato all'attività di foundraising, di comunicazione e informazione istituzionale e sviluppo di comunity
- finalizzato a rilevazioni statistiche e valutazione della didattica
- finalizzato al caso di diffusione dell'elaborato finale o di elementi ad esso connessi
- finalizzato a servizi di tutorato, assistenza, inclusione sociale
- finalizzato all'erogazione di servizi e attività per il diritto allo studio
- procedimenti di natura disciplinare a carico di studenti

Trattamenti inerenti a dipendenti e/o collaboratori:

- finalizzato allo svolgimento delle prove concorsuali
- finalizzato alla gestione del rapporto di lavoro
- finalizzato alla formazione e aggiornamento professionale

- finalizzato alla gestione di progetti di ricerca
- finalizzato al monitoraggio e alla valutazione della ricerca
- trattamenti nell'ambito di attività di trasferimento tecnologico
- trattamenti per politiche di welfare e per la fruizione di agevolazioni
- finalizzato alla salute e sicurezza delle persone nei luoghi di lavoro
    - trattamenti dell'ufficio Prevenzione, Protezione e Sicurezza
- finalizzato all'erogazione del servizio di telefonia fissa e mobile

Trattamenti trasversali o connessi ad attività trasversali:

- gestione degli spazi
- gestione delle postazioni di lavoro
- gestione degli organi e delle cariche istituzionali
    - finalizzato alla gestione degli elenchi per l'elettorato attivo e passivo
    - finalizzato alla nomina degli eletti e delle cariche accademiche
    - finalizzato alla pubblicizzazione di atti ai fini di trasparenza

Trattamento per la gestione degli infortuni

Trattamento in ambito bibliotecario

Trattamenti nell'ambito dei servizi di protocollo e conservazione documentale:

- finalizzato alla gestione del protocollo in entrata/uscita
- finalizzato alla conservazione documentale

Trattamenti per l'acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso:

- finalizzato all'acquisizione di beni e servizi
- finalizzato alle verifiche sull'espletamento di lavori, in cantiere o presso installazioni in Ateneo
- finalizzato alla gestione del contenzioso e del recupero crediti

Trattamenti nell'ambito dei servizi di posta elettronica e strumenti di collaboration:

- finalizzato all'accesso agli strumenti di collaboration
- finalizzato all'erogazione di servizi di posta elettronica

Trattamenti nell'ambito dell'erogazione federata di servizi:

- finalizzato all'erogazione del servizio Eduroam
- finalizzato all'accesso a servizi federati (es. IDEM)
- finalizzato all'accesso ai servizi con autenticazione SPID

Trattamenti relativi al tracciamento di informazioni non primarie:

- tracciamento sistemistico e di rete
- tracciamento applicativo

FAQ

1) Ho perduto lo smartphone su cui erano memorizzati messaggi di posta elettronica della mia casella UNIFI, 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.
2) 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.
3) Ho trovato che è stata forzata la serratura di un armadio contente archivi cartacei relativi alle carriere del personale tecnico amministrativo, ma sembra che non manchi nulla. Devo fare la segnalazione?
   La segnalazione è necessaria.
4) È stato rubato un notebook da un ufficio, nel quale erano contenuti dati personali. Devo fare la segnalazione?
   La segnalazione è necessaria.
5) Per errore ho inviato un messaggio di posta elettronica contenete una lista di studenti iscritti ad un corso con indicazione di matricola ed indirizzo e-mail a più destinatari sbagliati. Devo fare la segnalazione?
   La segnalazione è necessaria.
6) 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?
   Deve essere fatta la segnalazione.
7) 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 a al RPD. Se il responsabile non fosse reperibile rivolgersi al sostituto o al referente privacy se è stato nominato. In mancanza anche di questi contattare direttamente il Responsabile della protezione dati di Ateneo o il suo ufficio.

8) 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.