PROCEDURA PER LA GESTIONE DEL DATA BREACH

ai sensi del GDPR 2016/679, delle linee guida del WP29 e
delle indicazioni fornite dal Garante per la protezione dei dati personali

Indice

ALLEGATI:
101-MODULO DI SEGNALAZIONE VIOLAZIONE/SOSPETTO DATA BREACH
102-REGISTRO EVENTI NEGATIVI
103-SCHEMA DI VALUTAZIONE VIOLAZIONI-DATA BREACH

1. Premessa introduttiva

L'Università degli studi di Verona, quale Titolare del Trattamento ai sensi del Regolamento europeo 2016/679 (da qui in avanti GDPR), è tenuta a garantire la sicurezza dei dati personali trattati nell'ambito delle proprie attività e ad agire prontamente in caso di violazione dei dati stessi (come definito al punto 3).

L'Ateneo pianifica e mette in atto procedure idonee a rilevare e limitare tempestivamente gli effetti di una violazione, valutare il rischio per le persone fisiche e stabilire se sia necessario o meno notificare la violazione all'autorità di controllo competente e comunicarla alle persone fisiche interessate, ove necessario.

2. Scopo della procedura

Il presente documento ha lo scopo di indicare a tutti i soggetti che operano presso l'Ateneo le modalità di gestione di una violazione, anche solo potenzialmente ***data breach***, ovvero di un episodio di violazione di dati personali, nel rispetto dei principi e delle disposizioni contenute nel GDPR. Il presente documento è messo a disposizione di tutto il personale d'ateneo, attraverso la pubblicazione nella pagina intranet destinata ai servizi dell'UO Protezione Dati.

La procedura sintetizza le regole gestire nel migliore dei modi una violazione dei dati/*data breach*, sotto i diversi aspetti relativi a:

- Modalità e profili di segnalazione al Titolare;
- Valutazione dell'evento accaduto;
- Modalità e profili di segnalazione all'autorità Garante per la protezione dei dati personali (da qui in avanti Garante Privacy);
- Eventuale comunicazione agli interessati.

3. Violazione dei dati personali

Una violazione dei dati personali (o data breach), ovvero 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 (art. 4, punto 12 del GDPR) può, se non affrontata in modo adeguato e tempestivo, provocare **danni fisici, materiali o immateriali** alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Il data breach, o "violazione dei dati personali" nella traduzione italiana, è un concetto estremamente ampio.

Esso include certamente eventi in cui l'intervento malevolo di terzi è manifesto, ma comprende anche una serie di ipotesi riconducibili all'inosservanza di norme sulla sicurezza da parte del Titolare del trattamento. Tendenzialmente, il concetto di *data breach* viene a essere equiparato a quello di

rilevante discontinuità nel normale funzionamento di un sistema informatico.

Rientra nella categoria dei *data breach* anche un incidente sulla sicurezza dal quale deriva una perdita di disponibilità dei dati non permanente, ma circoscritta a un limitato periodo temporale, (ad esempio la perdita di accesso temporanea ai dati), in quanto potrebbe comunque comportare un significativo impatto sui diritti e le libertà degli individui (ad es. un blackout elettrico che impedisca all'interessato di accedere ai propri dati).

Anche la violazione che comporta la perdita temporanea di disponibilità **dovrebbe essere documentata** (così come nel caso di perdita o distruzione permanenti di dati personali); l'indisponibilità di un dato personale causata dalla manutenzione programmata del sistema in corso, non può essere considerata una "violazione della sicurezza" ai sensi del GDPR.

Le violazioni di dati personali possono essere ricondotte ad una serie di eventi tra cui:

- Divulgazione di dati personali a soggetti non autorizzati;
- Perdita o furto di dati o di strumenti nei quali sono memorizzati dati personali;
- Perdita o furto di documenti cartacei contenenti dati personali;
- Infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia per fini non consentiti);
- Accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- Casi di pirateria informatica (usurpazione delle credenziali di accesso – phishing – ransomware);
- Banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- Virus o altri attacchi al sistema informatico o alla rete aziendale;
- Violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o armadi contenenti archivi con informazioni riservate);
- Smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- Invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

Per gestire tali data breach, occorre seguire le disposizioni di seguito descritte.

4. Soggetti tenuti all'osservanza della procedura

La procedura si rivolge a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza dell'Ateneo, quali i lavoratori dipendenti, nonché coloro che, a prescindere dall'inquadramento contrattuale in essere, abbiano accesso ai dati per garantire l'esecuzione delle prestazioni richieste.

5. Gestione del *data breach*

Le violazioni di dati personali sono gestite operativamente dall'UO Protezione Dati dell'Area Trasparenza e Protezione Dati – Direzione Affari Istituzionali, sotto la supervisione del Responsabile

della Protezione dei Dati (da qui in avanti DPO).

Ogni soggetto autorizzato a trattare dati, qualora venga a conoscenza di un potenziale caso di *data breach*, è tenuto ad informare tempestivamente il Titolare, compilando l'apposito modulo **101-MODULO DI SEGNALAZIONE VIOLAZIONE/SOSPETTO DATA BREACH** (da qui in avanti MODULO 101) ed inviandolo all'Ufficio Protezione Dati, all'indirizzo di posta elettronica: privacy@ateneo.univr.it.

La segnalazione ricevuta sarà valutata in ordine a stabilire il possibile rischio per gli interessati e successivamente annotata nell'apposito registro: **102-REGISTRO EVENTI NEGATIVI** (da qui in avanti REGISTRO 102).

Si possono presentare le **tre seguenti situazioni**:

A. **improbabilità che la violazione dei dati personali verificatasi presenti un rischio per i diritti e le libertà delle persone fisiche:** In tal caso è necessario acquisire la segnalazione (MODULO 101) e conservarne menzione nel registro (REGISTRO 102) indicando le motivazioni per cui si è deciso di non procedere con la notifica al Garante.

B. **probabilità che la violazione dei dati personali verificatasi presenti UN RISCHIO per i diritti e le libertà delle persone fisiche:** In tal caso è obbligatoria apposita notifica al Garante.

   In tal caso di rischi è necessario effettuare la notifica entro 72 ore, tramite **l'apposita procedura telematica resa disponibile dal Garante** nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/[1].

C. **probabilità che la violazione dei dati personali verificatasi presenti un RISCHIO ELEVATO per i diritti e le libertà delle persone fisiche**: è necessario procedere immediatamente alla comunicazione agli interessati, oltre alla notifica al Garante Privacy entro 72 ore.

Al fine di classificare correttamente l'incidente incorso e valutare l'entità del rischio conseguente, l'Ufficio Protezione Dati potrà utilizzare il documento allegato alla presente procedura: **103-SCHEMA DI VALUTAZIONE VIOLAZIONI-DATA BREACH** (da qui in avanti SCHEMA 103).

Il criterio dirimente per valutare la necessità di avviare una procedura di notifica è la probabilità che la violazione possa porre a rischio (per la notifica all'autorità – Garante Privacy) o a rischio elevato (per la comunicazione anche agli interessati) le libertà e i diritti degli individui.

Appurato il rischio conseguente alla violazione, gli artt. 33 e 34 del GDPR indicano al Titolare i termini, le modalità, i contenuti e le deroghe della notifica e della comunicazione di *data breach*.

Pertanto, affinché la violazione dei dati personali sia gestita correttamente, è necessario seguire i seguenti step:

1) Identificazione della violazione ed avvio delle azioni correttive per gestire la violazione;
2) Indagine su quanto avvenuto e valutazione del rischio per gli interessati con annotazione nell'apposito registro;
3) Eventuale notifica all'Autorità Garante;
4) Eventuale comunicazione agli interessati;

[1] Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante.

5) Documentazione della violazione indipendentemente dall'esito della valutazione.

5.1 Identificazione della violazione ed avvio delle azioni correttive per gestire la violazione

Rilevata la violazione si richiede alle competenti strutture di Ateneo di porre in essere, se possibile, azioni correttive atte a limitare i danni cagionati e di compilare il MODULO 101, informando i soggetti preposti alla gestione delle violazioni dei dati (Ufficio Protezione Dati, che attiverà il DPO in base all'urgenza) dell'avvenuto incidente.

Soggetti esterni all'Ateneo possono comunque segnalare presunte violazioni di dati personali, di cui siano accidentalmente venuti a conoscenza, utilizzando direttamente il MODULO 101, disponibile on line: www.univr.it/privacy.

Qualora la segnalazione provenga da Responsabili del trattamento ex art. 28 del GDPR, l'Ateneo ricorda che i contratti in essere tra il Titolare e tutti i Responsabili del trattamento individuati, prevedono l'obbligo, in capo al Responsabile, di informare tempestivamente il Titolare in caso di violazione.

Il MODULO 101 è messo a disposizione secondo le modalità indicate nella seguente tabella.

SEGNALANTI DATA BREACH INTERNI	**DISPONIBILITÀ MODULO 101**	
	Sito *(www.univr.it/privacy)*	**Intranet** *(MyUnivr)*
Utenza esterna *(cittadini, partecipanti ai convegni, studenti scuole superiori, utenti dei siti web d'Ateneo, visitatori, etc.)*	√	
Studenti e studentesse dell'Ateneo	√	√
Personale (docente e TA) dell'Ateneo	√	√

5.2 Indagine su quanto avvenuto e valutazione del rischio per gli interessati

Ricevuta la segnalazione l'Ufficio Protezione Dati, al fine di stabilire se si sia effettivamente verificata un'ipotesi di *data breach* procede ad indagini approfondite sull'accaduto, coinvolgendo anche il DPO se necessario.

Tale indagine verrà condotta sulle base delle informazioni raccolte nel MODULO 101, compilato da chi ha rilevato la violazione e/o da eventuali testimoni. Sulla base di tali informazioni, l'Ufficio Protezione Dati, con il coinvolgimento del DPO in base all'urgenza, effettua la prevista valutazione di rischio per i diritti e le libertà dei soggetti interessati.

Nel valutare il rischio, verranno considerate le circostanze specifiche della violazione, inclusa la

gravità dell'impatto potenziale e la probabilità che tale impatto si verifichi. A tal fine, saranno considerati i seguenti parametri: tipo di violazione, natura e volume dei dati personali violati, facilità di identificazione delle persone fisiche e caratteristiche particolari dell'interessato.

Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, l'Ufficio Protezione Dati coinvolgerà immediatamente il Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni, o un suo delegato in caso di assenza, e le competenti strutture del servizio informatico d'Ateneo, tenuto conto anche delle adottate procedure di sicurezza informatica.

A fronte di tale analisi, l'Ateneo, tramite l'ufficio Protezione Dati, in collaborazione col DPO, accerterà:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (ad esempio riparazione fisica degli strumenti; utilizzo dei file di backup per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso, etc.)
- una volta identificate tali azioni, quali siano le strutture d'Ateneo che devono agire per contenere la violazione
- se sia necessario notificare la violazione al Garante (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche)
- se sia necessario comunicare la violazione anche agli interessati (ove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche).

Al fine di valutare la necessità di effettuare la segnalazione al Garante Privacy e agli interessati, l'Ateneo, tramite l'ufficio Protezione Dati, in collaborazione col DPO, utilizzerà lo SCHEMA 103.

Qualora la valutazione del rischio dia esito negativo e i soggetti preposti alla gestione dell'incidente, non ritengano necessaria la segnalazione all'autorità di controllo, si terrà ugualmente traccia di quanto avvenuto attraverso la compilazione del REGISTRO 102, specificando i motivi per cui non si ritiene di procedere con la segnalazione di Data Breach.

L'Ateneo, qualora si trovasse ad operare come Responsabile, si impegna a rispettare quanto sopra indicato nei confronti delle controparti che ci hanno designato loro Responsabile del trattamento in base ai contratti/accordi/convenzioni in essere, stabilendo in 48 ore il tempo massimo per informare il Titolare a partire dal momento della scoperta della violazione, salvo diverso accordo stipulato.

5.3 Eventuale notifica al Garante Privacy

Una volta valutata la necessità di effettuare notifica della violazione dei dati subita, l'Ateneo, tramite l'ufficio Protezione Dati, in collaborazione col DPO, predispone la segnalazione e la invia all'Autorità Garante, senza ingiustificato ritardo e, comunque, **entro 72 ore** dal momento in cui si è venuti a conoscenza della violazione, cioè da quando si abbia un ragionevole grado di certezza di un avvenuto incidente di sicurezza che riguardi dati personali.

Per l'invio della notifica, verrà utilizzata l'apposita procedura telematica resa disponibile dal Garante nel portale dei servizi online dell'Autorità (https://servizi.gpdp.it/databreach/s/).

L'Ateneo è tenuto a valutare le circostanze specifiche di ogni effettiva violazione avvenuta. Pertanto, qualora non disponga di tutti gli elementi di dettaglio dell'incidente, è tenuto comunque ad

effettuare la notifica della violazione al Garante entro 72 ore, con le informazioni in suo possesso, classificando come preliminare la notifica effettuata. Una volta ricostruito il quadro completo della violazione l'Ateneo provvederà alla compilazione del medesimo modulo, individuando come integrativa la notifica in essere.
L'Ateneo, tramite l'ufficio Protezione Dati, curerà l'archiviazione della documentazione riguardante la violazione in modo regolare e puntuale, anche durante il suo sviluppo, così da raccogliere le informazioni necessarie e tutti i dettagli rilevanti, tenute a disposizione dell'Autorità Garante.
Nell'ipotesi in cui la segnalazione sia effettuata oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.
La **notifica al Garante** non includerà i dati personali oggetto di violazione (es. i nomi dei soggetti interessati dalla violazione). Viceversa, la **notifica,** ai sensi dell'art. 33, par. 3, GDPR, indicherà:

- Tipo di notifica: se è preliminare (l'Ateneo avvia il processo di notifica pur in assenza di un quadro completo della violazione con riserva di effettuare notifica integrativa), completa o integrativa;
- Generalità del soggetto che effettua la notifica e dati dell'Ateneo;
- Riferimenti del soggetto da contattare per ottenere informazioni aggiuntive inerenti la violazione (DPO, Responsabile del trattamento, altri soggetti coinvolti);
- Informazioni di sintesi sulla violazione: indicazioni temporali della violazione, modalità in cui l'Ateneo è venuto a conoscenza dell'incidente, motivi del ritardo della segnalazione;
- Descrizione della violazione: natura della violazione (perdita di confidenzialità, perdita di integrità, perdita di disponibilità), cause della violazione (azione intenzionale interna, azione accidentale interna, azione intenzionale esterna, azione accidentale esterna o causa sconosciuta), categorie di dati personali oggetto di violazione (dati anagrafici, dati di contatto, dati di accesso e di identificazione, dati di pagamento, dati relativi alla fornitura di un servizio di comunicazione elettronica, dati di profilazione, dati giudiziari, dati di localizzazione, dati relativi a documenti di identificazione/riconoscimento, dati particolari), volume dei dati raccolti, categorie di interessati coinvolti (dipendenti/consulenti, utenti, contraenti/abbonati, clienti attuali o potenziali, associati/soci/aderenti, soggetti che ricoprono cariche sociali, beneficiari o assistiti, pazienti, minori, persone vulnerabili, etc.);
- Informazioni di dettaglio sulla violazione: indicazione delle infrastrutture IT coinvolte e loro ubicazione, misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei sistemi e delle infrastrutture IT coinvolte;
- Probabili conseguenze della violazione dei dati (i dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento, i dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito, i dati sono stati modificati e resi inconsistenti, malfunzionamento e difficoltà nell'utilizzo di servizi, etc.);
- Potenziali effetti negativi per gli interessati (perdita del controllo dei dati, limitazione dei diritti, discriminazione, furto o usurpazione d'identità, frodi, perdite finanziarie, decifratura non autorizzata delle pseudonimizzazione, pregiudizio alla reputazione, danno economico o sociale significativo, etc.);
- Eventuali misure adottate dall'Ateneo per porre rimedio o attenuare l'infrazione e per prevenire simili violazioni future;
- Comunicazione agli interessati (ragioni dell'avvenuta/mancata comunicazione, numero degli

interessati a cui è stata trasmessa, contenuto della comunicazione, canale utilizzato);

- Altre informazioni (comunicazioni ad altre autorità di controllo, ad organismi di vigilanza o di controllo, all'autorità giudiziaria o di polizia, indicazione dell'appartenenza dei paesi coinvolti allo Spazio Economico Europeo).

5.4 Eventuale comunicazione agli interessati

Accanto agli obblighi di notifica all'autorità di controllo, l'art. 34 GDPR prevede in capo ai titolari un obbligo di comunicazione della violazione, **senza ingiustificato ritardo**, all'interessato per consentirgli di attivarsi a tutela dei propri interessi.

La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione.

Tale comunicazione all'interessato **non è richiesta** se:

- Il Titolare del trattamento ritiene che la violazione dei dati personali non presenti un rischio elevato per i diritti e le libertà delle persone fisiche;
- Il Titolare del trattamento ha messo in atto misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;
- Il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- Detta comunicazione richiederebbe sforzi sproporzionati. In tale caso, si procede invece a una comunicazione pubblica o a una misura simile.

Nell'eventualità in cui l'Ateneo si trovi nell'impossibilità di contattare il soggetto interessato dal *data breach*, in quanto non dispone delle informazioni necessarie per riuscire a mettersi con questo in contatto, effettuerà la comunicazione non appena sia ragionevolmente possibile farlo (ad es. qualora il singolo esercitando il proprio diritto di accedere ai dati personali, ai sensi dell'articolo 15 GDPR, fornisca all'Università le informazioni supplementari necessarie per contattarlo).

La comunicazione deve essere distinguibile dalle altre trasmesse agli interessati, in altri termini, **la comunicazione deve essere chiara, inequivocabile e richiamare l'attenzione dell'interessato**. Pertanto, l'Ateneo eviterà di trasmettere la comunicazione nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintese dai lettori; solo qualora la segnalazione diretta richieda sforzi sproporzionati, la normativa consente all'Ateneo di effettuare una comunicazione pubblica a patto che mantenga lo stesso grado di efficacia conoscitiva del contatto diretto con l'interessato. Così, mentre può ritenersi adeguata la comunicazione fornita attraverso evidenti banner o notifiche disposte sui siti web, non lo sarà se questa sia limitata all'inserimento della notizia in un blog o in una rassegna stampa: l'adeguatezza di una comunicazione è quindi determinata non solo dal contenuto del messaggio, ma anche dalle modalità di effettuazione.

La **comunicazione agli interessati,** ai sensi dell'art. 34, par.3, GDPR, comprenderà:

- una descrizione generale della violazione dei dati (natura della violazione, categorie e numero approssimativo di interessati nonché categorie e numero approssimativo di dati

personali coinvolti);

- nome e dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati;
- descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali.

5.5 Documentazione della violazione indipendentemente dal suo esito.

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di *data breach*, ogni qualvolta si verifichi un incidente, occorre archiviare la documentazione relativa, in virtù di quanto disposto dall'art. 33, par. 5, GDPR, nel rispetto del principio di responsabilizzazione, tenendo l'archivio a disposizione dell'Autorità Garante. L'Ateneo, per il tramite dell'Ufficio Protezione Dati, provvede alla compilazione e all'aggiornamento del REGISTRO 102.

Nel GDPR non è specificato un periodo di conservazione per tale tipologia di documentazione. Laddove tali registrazioni contengano dati personali, spetta all'Ateneo determinare il periodo adeguato di conservazione, in conformità ai principi applicabili al trattamento dei dati personali, e individuare la corretta base legale per svolgere tale trattamento; tale documentazione potrebbe peraltro risultare idonea prova di conformità alla normativa vigente.

Qualora i "Data Breach record" non contengano dati personali, il principio di limitazione della conservazione del GDPR non si applica.

6. Ruolo del DPO

In termini di documentazione delle violazioni, il Titolare del trattamento o il Responsabile del trattamento devono richiedere il parere del proprio DPO in merito alla struttura, all'impostazione e all'amministrazione di tale documentazione.

Il DPO svolge un *ruolo chiave* nell'assistenza alla prevenzione delle violazioni, fornendo consulenza e monitorando la conformità delle procedure e delle azioni poste in essere, nonché nel corso di notifica all'Autorità Garante e durante qualsiasi successiva indagine da parte della stessa.

Pertanto, l'Ateneo informa tempestivamente il proprio DPO dell'esistenza di una violazione, coinvolgendolo durante la gestione delle violazioni ed il processo di notifica.