UNIVERSITÀ DEGLI STUDI DI BRESCIA

DECRETO

Oggetto: Adozione "PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (*Personal Data Breach*)"

IL RETTORE

VISTO il D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" s.m.i.;

VISTO il Regolamento UE 2016/679 - GDPR (*General Data Protection Regulation*) - del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, in particolare l'art.33;

VISTA la Legge 25 ottobre 2017, n. 163 di delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del GDPR;

VISTI i Provvedimenti del Garante della Privacy italiano del 30 luglio 2019 e del 21 maggio 2021;

VISTO il D.R. n.1355/2021, prot.156330, con cui Frareg s.r.l. (C.F. e P. IVA 11157810158) è stato designato quale Responsabile della Protezione Dati (*Data Protection Officer – RPD/DPO*) per l'Università degli Studi di Brescia per il periodo dal 23 dicembre 2021 al 22 dicembre 2022;

VISTO il D.R. n.535/2022, prot.213316, relativo alla "Nomina dei referenti del Responsabile della protezione dei dati (RPD) per l'attuazione del Regolamento UE 2016/679 – GDPR";

CONSIDERATO che per «violazione dei dati personali» (*data breach*) si intende la 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; art. 2, comma 1, lett. m, del D.Lgs. n. 51/2018);

CONSIDERATO, altresì, che la violazione dei dati personali (*data breach*) costituisce un rischio per i diritti e la libertà delle persone fisiche (artt. 33, 34 e 55 del GDPR, art. 2-bis del Codice) e, qualora si verifichi, il titolare del trattamento è tenuto, ai sensi di quanto previsto dal GDPR, a:

- notificare l'eventuale violazione dei dati personali al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza;
- notificare la violazione dei dati personali al Garante con le modalità di cui all'art. 33 del GDPR anche con riferimento al trattamento effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvo che il trattamento medesimo sia effettuato dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del Pubblico Ministero (artt. 26 e 37, comma 6, del D.Lgs. n. 51/2018);
- comunicare la violazione all'interessato senza ingiustificato ritardo quando essa è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

PRECISATO che la omessa notifica di *data breach* all'Autorità di controllo - oltre a costituire un possibile danno per i soggetti interessati - è punita con l'irrogazione di sanzioni amministrative a carico del titolare del trattamento;

VALUTATA la necessità di adottare una procedura interna per la corretta ed efficace gestione delle violazioni dei dati personali - (*Personal Data Breach*) che disciplini puntualmente la prassi da seguire nell'eventualità che si verifichi un evento rischioso;

VISTA la procedura predisposta dal Responsabile della Protezione Dati "PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (*Personal Data Breach*)" (all.1) in cui sono previsti i compiti e le attività da porre in essere entro le 72 ore dal verificarsi dell'evento e la definizione di un modulo da utilizzare per la segnalazione delle violazioni riscontrate;

ATTESA altresì l'esigenza che la stessa procedura sia adeguatamente diffusa e portata all'attenzione di tutti i dipendenti dell'Ateneo affinché venga adottata da ciascuno per la parte di competenza;

DECRETA

per le motivazioni indicate nelle premesse del presente atto e che qui si intendono integralmente riportate,

- di adottare la "PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (*Personal Data Breach*)" (all.1), parte integrante e sostanziale del presente provvedimento;
- di dare massima diffusione alla stessa.

Brescia, *data del protocollo*

IL RETTORE
(Prof. Maurizio Tira)
Documento firmato digitalmente ex art. 24 D. Lgs 82/05

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

(*Personal Data Breac*h)

Art. 33 Regolamento (UE) 2016/679 e
Art. 26 D.Lgs. 51/2018
Provvedimento del Garante della Privacy italiano
del 30 luglio 2019 e del 21 maggio 2021

	Struttura	Nome
Redatto da:	Staff RPD	Renato Veronesi, Antonio Zuccaro, Stefano Filippini
	Responsabile "Servizi ICT"	Andrea Marinoni
	Responsabile della Protezione dei Dati (RPD)	Frareg S.r.l.
Verificato da:	Direttrice Generale	Loredana Monica Elisabetta Luzzi
Approvato da:	Rettore	Maurizio Tira

Cronologia delle Revisioni

Revisione	Data	Sintesi delle Modifiche
01	16/06/2022	Prima versione consolidata

Livello di riservatezza
Il documento deve essere reso disponibile al personale di **Università degli Studi di Brescia** e ai soggetti esterni che la stessa ritenga opportuno siano informati.

Indice

1.1 Introduzione

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, **Università degli Studi di Brescia** quando agisce in qualità di titolare del trattamento e/o di responsabile del trattamento si impegna a mettere in atto tutte le misure tecniche e organizzative più adeguate al fine di garantire un livello di sicurezza adeguato ai rischi legati ad ogni tipologia di trattamenti dei dati personali degli interessati.

Università degli Studi di Brescia nel pieno rispetto delle normative cogenti, nazionali e sovranazionali, si impegna a proteggere i dati personali, a mantenerli al sicuro e a rispondere tempestivamente e adeguatamente alle violazioni di dati (compresa, in alcuni casi, la segnalazione di tali violazioni al Garante per la Protezione dei Dati e, se del caso, anche ai soggetti coinvolti). È fondamentale che vengano adottate azioni tempestive in caso di violazioni di dati effettive, potenziali o sospette, per evitare il rischio di danni agli individui, danni operativi e gravi costi finanziari, legali e di reputazione nei riguardi dell'Ateneo.

1.2 Finalità e Scopo

Lo scopo di questo documento è fornire informazioni generali sul tema del data breach e istruzioni operative da utilizzare per la segnalazione e la gestione di eventuali violazioni di dati[1] che riguardino i dati personali o "particolari" (definiti di seguito) trattati da **Università degli Studi di Brescia**. Queste procedure sono un supplemento alla Politica di protezione dei dati adottata da **Università degli Studi di Brescia**, la quale afferma il suo impegno a tutelare il diritto alla privacy degli individui in conformità con la legislazione nazionale ed Europea sulla protezione dei dati personali in vigore.

1.3 Ambito di applicazione

Il presente documento si applica ai processi che si attivano in caso di violazione dei dati personali dei quali **Università degli Studi di Brescia** risulti essere il Titolare e/o Responsabile del trattamento, al fine di rilevare e limitare tempestivamente gli effetti di una violazione dei dati personali, svolgere la valutazione del rischio per le persone fisiche e di conseguenza a ponderare, ove necessario, la notificazione della violazione all'autorità di controllo competente e la comunicazione della medesima alle persone fisiche interessate.

1.4 Definizioni

Si riportano di seguito le definizioni dei concetti di maggior rilievo ai fini di una miglior comprensione dell'applicazione nell'ambito dell'**Università degli Studi di Brescia** della seguente *Procedura di gestione e notifica di Violazione di Dati personali*:

GDPR: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione

Dato personale - qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Interessato: qualsiasi persona fisica i cui dati personali vengono trattati (da un Titolare o da un Responsabile del trattamento)

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali

Responsabile (esterno) del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

Violazione di dati personali (o *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.

Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro per sorvegliare l'applicazione del GDPR al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e per agevolare la libera circolazione dei dati personali all'interno dell'UE.

Responsabile della protezione dei dati: soggetto designato all'interno dell'Ateneo, ai sensi dell'articolo 37 del GDPR, responsabile dell'osservanza dei requisiti del GDPR e delle politiche in materia di protezione dei dati, assolvendo alle funzioni di vigilanza e consulenza nei confronti del Titolare del trattamento.

Referente del RPD E' la persona di riferimento del RPD per ogni Dipartimento ed articolazione amministrativa all'interno dell'Ateneo.

Servizio "Servizi ICT": gestore dei servizi informatici d'Ateneo.

Incidente: evento imprevisto, improvviso, indesiderato e inatteso, che può essere causa di un danno (alle cose, alle persone o ai dati trattati)

1.5 DEFINIZIONE VIOLAZIONE DEI DATI PERSONALI (*DATA BREACH*)

Il *Data Breach* è definito dall'art. 4 del GDPR come una "**violazione della sicurezza"** che comporta la illecita e/o accidentale distruzione, perdita, modifica, rivelazione non autorizzata o accesso ai dati personali trasmessi, memorizzati e in ogni caso trattati.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità e/o la disponibilità di dati personali.

Possono essere identificate differenti tipologie di *Data Breach*:

1) **"*Confidentiality Breach*"** ovvero un accesso non autorizzato ai dati personali;
2) **"*Availability Breach*"** ovvero la perdita degli accessi, o la cancellazione, di dati personali;
3) **"*Integrity Breach*"** ovvero un'alterazione non autorizzata o accidentale dei dati personali

Alcuni possibili esempi di Data Breach:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Un *Data Breach* può dar luogo a conseguenze negative sugli interessati che possono causare danni materiali, non materiali e/o fisici. Il Regolamento UE sulla protezione dei dati personali, più precisamente negli art.33 e ss., spiega come queste conseguenze possano includere, per esempio, la perdita del controllo sui propri dati personali, la limitazione dei propri diritti, operare una discriminazione, un furto di identità o frode, delle perdite economiche, un danno alla reputazione, la perdita della confidenzialità dei dati protetti da segreto professionale etc.

1.6 COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI

1.6.1 DOVERI DEL TITOLARE DEL TRATTAMENTO

Il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia **improbabile** che la violazione dei dati personali comporti un **rischio** per i diritti e le libertà delle persone fisiche.

Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere **accompagnate dai motivi del ritardo.**

Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il Titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

Il titolare del trattamento, a prescindere dalla notifica al Garante, **documenta** tutte le violazioni dei dati personali, ad esempio predisponendo un apposito registro (attualmente all'interno del software GDP). Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

1.6.2 FIGURE INTERNE COINVOLTE E RESPONSABILITÀ

Di seguito si riportano in schema, le figure generalmente coinvolte all'interno dell'organizzazione al fine di gestire correttamente la violazione dei dati.

RUOLO	RESPONSABILITÀ
DIPENDENTE	• **Si attiene alle indicazioni di Ateneo e alle istruzioni del Servizio "Servizi ICT" in materia di protezione dei dati personali al fine di prevenire e contenere i danni di un possibile Data Breach.** • Segnala, tempestivamente, al RPD, al referente RPD e ai servizi ICT qualunque evento/incidente che possa comportare la perdita di integrità, disponibilità o riservatezza dei dati personali, mediante specifico form disponibile sul portale di ateneo.
REFERENTE DEL RPD	• Riceve le segnalazioni dei dipendenti di riferimento in condivisione con l'RPD ed i servizi ICT. • Segnala eventuali eventi/incidenti di cui sia venuto direttamente a conoscenza mediante lo specifico form disponibile sul portale di ateneo. • Partecipa, insieme ai suddetti soggetti, alle riunioni di analisi dell'evento segnalato, al fine di classificarlo come possibile data breach o meno**.**
SERVIZI ICT	• Riceve le segnalazioni, in condivisione con l'RPD e il referente del RPD. • Rileva le segnalazioni dai sistemi di monitoraggio della sicurezza e da quelli di prevenzione delle intrusioni - *Intrusion Detection Prevention* (IDP), software antivirus, sistemi di monitoraggio dei log, ovvero dai sistemi di monitoraggio della rete come firewall, sistemi di analisi del flusso di rete e filtraggio web. • Mette in sicurezza il sistema. • Collabora con l'RPD nella valutazione della gravità del *Data Breach* e nella predisposizione del modello per la notifica al Garante.
RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)	• Riceve le segnalazioni, in condivisione con il referente del RPD e i servizi ICT. • Indice e coordina la riunione di analisi dell'evento. • Analizza l'evento segnalato al fine di classificarlo come possibile data breach o meno avvalendosi della collaborazione dei suddetti soggetti. • Predispone nei tempi previsti dalla normativa l'eventuale notifica al Garante. • Valuta l'opportunità di segnalazione del *Data Breach* ai soggetti interessati. • Recepisce le indicazioni del Garante inerenti il *Data Breach* e le comunica alle funzioni interessate. • Registra l'evento nell'apposito Registro degli incidenti (all'interno del software GDP).

TITOLARE DEL TRATTAMENTO	• Collabora con l'RPD e il Servizio "Servizi ICT" nella valutazione dell'entità del *Data Breach*. • Valuta la necessità di comunicare il *Data Breach* ai soggetti interessati con il supporto del RPD.
SOGGETTO ESTERNO (ES. FORNITORE, COLLABORATORE, UTENTE, ETC.)	• Segnala, tempestivamente, al RPD, al referente RPD e ai servizi ICT qualunque evento/incidente che possa comportare la perdita di integrità, disponibilità o riservatezza dei dati personali, mediante specifico form disponibile sul portale di ateneo.
STRUTTURA DI SUPPORTO AL RESPONSABILE DELLA PROTEZIONE DEI DATI (STAFF RPD)	• Collabora con l'RPD e il Titolare del trattamento. • Fornisce supporto alle strutture coinvolte nell'incidente al fine di ottemperare alle disposizioni del GDPR.

1.6.3 DOVERI DEL RESPONSABILE DEL TRATTAMENTO

Il Responsabile del trattamento che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare del trattamento ai sensi dell'art. 33 del GDPR. La mancata comunicazione della violazione potrebbe causare danni economici al Titolare del trattamento dei dati.

1.6.4 POSSIBILI SCENARI

L'incidente e/o la violazione può avvenire:

1.6.4.1 Internamente all'Organizzazione (a titolo esemplificativo):

- quando riguarda un fatto accaduto ad un dipendente o collaboratore relativamente a dati, documenti o dispositivi dell'organizzazione;
- quando si notano anomalie nel funzionamento degli strumenti informatici di lavoro, siti internet, applicazioni software, si ricevono e-mail sospette da mittenti sconosciuti, o potenzialmente conosciuti che inducono a rilevare informazioni, od effettuare azioni quali cliccare su determinati link, siti, pulsanti, etc.;
- quando si è impossibilitati ad accedere ai dati;
- quando si ricevono e-mail e/o messaggi (SMS, WhatsApp, etc.) da soggetti conosciuti che ordinano disposizioni insolite da effettuarsi immediatamente;
- quando si ricevono telefonate da soggetti sconosciuti che cercano di estorcere informazioni dell'organizzazione o da soggetti conosciuti che ordinano disposizioni insolite da effettuarsi immediatamente;
- quando si ha il sospetto che i documenti o gli archivi cartacei siano stati comunicati o diffusi a soggetti non autorizzati.

1.6.4.2 Esternamente all'Organizzazione (a titolo esemplificativo):

- quando riguarda un fatto accaduto ad un dipendente o collaboratore relativamente ad un furto o smarrimento di uno strumento elettronico (tablet, smartphone, notebook, dispositivi esterni di memorizzazione USB, etc.) dell'organizzazione, o di un documento o archivio cartaceo potenzialmente contenenti dati ed informazioni, di cui è titolare l'Università degli studi di Brescia;
- quando riguarda un fatto accaduto ad un fornitore (consulenti, professionisti, servizi di informatica, etc.), ad un utente, o a qualsiasi soggetto legato da un rapporto con l'Università degli studi di Brescia che tratta dati della medesima o da questa gestiti;

- quando si ha il sospetto che documenti o archivi cartacei siano stati comunicati o diffusi a soggetti non autorizzati.

1.6.4.3 A seguito di comunicazioni da organi di stampa o dell'Autorità Garanti:

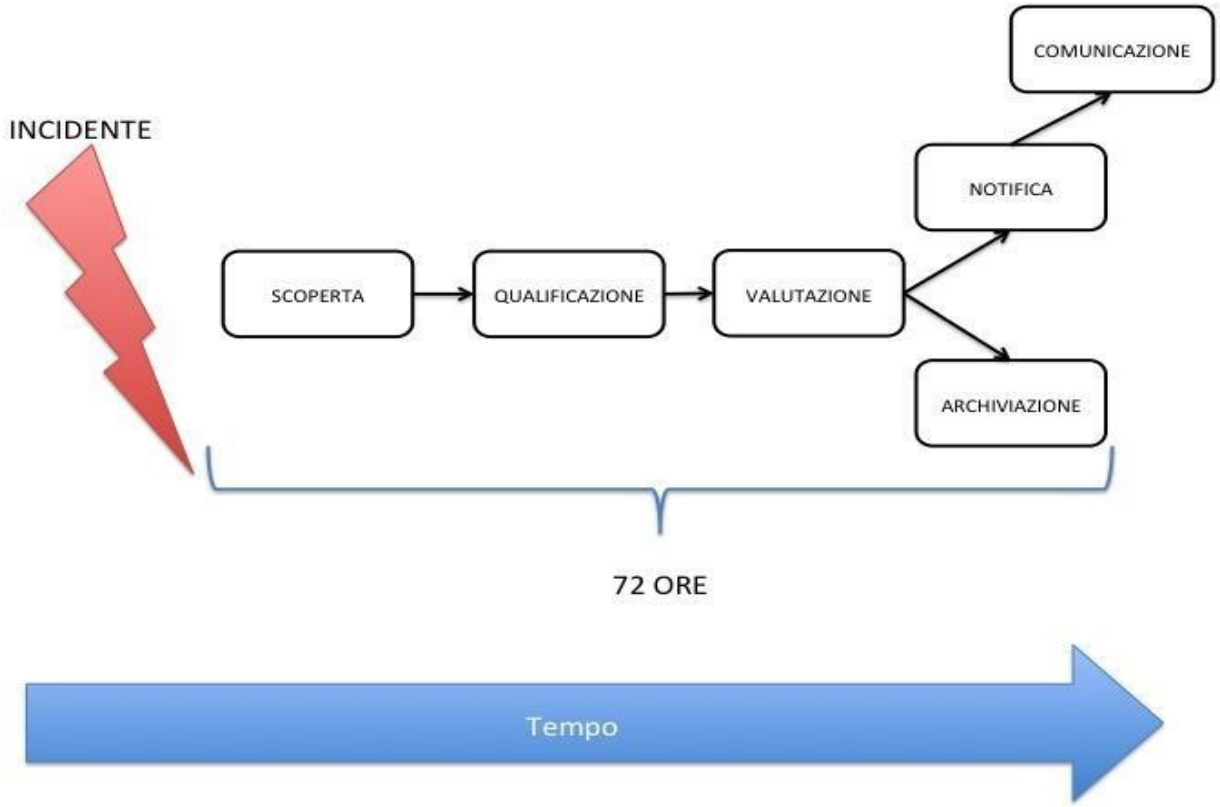
- quando si ha notizia di violazioni di dati personali da parte degli organi di stampa (attendibili) in merito a piattaforme cloud pubbliche, private, o da parte di fornitori di servizi di informatica, telefonia, internet, servizi pubblici, poste, Enti ed organi dello Stato, etc., con le quali risultano in essere rapporti diretti o indiretti con l'Università degli studi di Brescia;
- quando si ha notizia da parte di una delle Autorità Garante nazionale o di un altro Paese europeo, (od extra europeo) di una violazione di dati.

1.7 COME COMPORTARSI - PROCEDURA DI ATENEO PER LA GESTIONE DELLA VIOLAZIONE:

Di seguito si riportano due schemi esemplificativi di quanto richiesto dalla normativa per la corretta gestione della violazione:

1.7.1 Schema 1

Il presente grafico vuole evidenziare la durata o l'arco temporale nel quale deve svolgersi la valutazione e l'eventuale notifica all'Autorità Garante dell'avvenuto *Data Breach*.



1.7.2 Fase 1: segnalazione

La rilevazione e la segnalazione dell'incidente è un obbligo di tutti i dipendenti e/o collaboratori che possono effettuarla attraverso lo specifico form.

In caso di emergenza, non si riuscisse ad utilizzare lo specifico form, è comunque necessario inviare tempestivamente una mail a rpd@unibs.it al fine di consentire di notificare l'eventuale data breach al Garante entro le tempistiche richieste dalla normativa.

1.7.3 Fase 2: analisi e messa in sicurezza

Primo step: Ricevuta la segnalazione da un dipendente o un qualsivoglia soggetto o rilevata un'anomalia di sistema, in modo condiviso, l'RPD, il referente RPD e il servizio "Servizi ICT" procedono con l'analisi della segnalazione e valutano se l'incidente ha comportato la perdita, la modifica o la divulgazione di dati personali afferenti a persone fisiche.

Secondo Step: Effettuata la valutazione, il suddetto gruppo di lavoro redigerà un *Report* al fine di dar conto al Titolare della gravità della violazione ed incidenza sulla riservatezza, integrità e disponibilità dei dati.

Terzo step: A seguito dell'analisi effettuata, l'RPD riporta nel Registro dei *Data Breach* (all'interno del software GDP) l'evento. Il Registro ha funzione di archivio storico degli incidenti sui dati.

Eseguiti i precedenti passaggi, il suddetto gruppo di lavoro dovrà qualificare l'incidente accaduto, seguendo la classificazione che segue:

a. l'incidente non comporta alcuna violazione: deve, quindi, semplicemente essere riportato nel Registro degli incidenti (all'interno del software GDP);
b. l'incidente comporta una violazione dei *Personal Data*: nel caso in cui la violazione interessi l'ambito informatico, si attiverà la procedura descritta nel paragrafo seguente.

- ***Procedura di gestione e mitigazione della violazione dei dati personali in ambito informatico:***

Il Servizio "Servizi ICT" provvederà immediatamente alla messa in sicurezza delle aree (fisiche e/o virtuali) impattate, isolando, ove possibile, l'Incidente e verificando:

a) la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il volume approssimativo di dati personali oggetto di violazione;
b) le probabili conseguenze derivanti dalla violazione dei dati personali;
c) le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento (contromisure tecniche per la mitigazione del rischio cyber), per porre rimedio alla violazione dei dati personali e, se del caso, al fine di mitigare i possibili effetti negativi, provvedere alla comunicazione delle predette informazioni, contestualmente, al Titolare del trattamento ed al reparto amministrativo.

Analoghe cautele (contromisure a carattere fisico ed organizzativo) dovranno essere assunte, in quanto compatibili, qualora l'incidente di sicurezza non abbia natura digitale, ma incida, in ogni caso, su disponibilità, integrità o riservatezza dei dati personali dei quali l'Ateneo risulti essere Titolare del trattamento.

Qualora risulti che dai primi elementi acquisiti la responsabilità dell'incidente informatico o di sicurezza sia ragionevolmente ascrivibile ad uno degli utenti abilitati ad accedere al sistema informativo di Ateneo, il Servizio "Servizi ICT", previa autorizzazione per le vie brevi del management, provvede ad inibire l'accesso al sistema dell'utente sospettato d'essere responsabile dell'abuso dei propri privilegi d'accesso.

REGISTRO DEGLI INCIDENTI

Il registro degli incidenti è conservato ed aggiornato a carico di:

RUOLO	E-MAIL
Responsabile della Protezione dei Dati -R.P.D.	rpd@unibs.it

1.7.4 Fase 3: valutazione sull'impatto privacy

L'RPD e il relativo referente, con l'eventuale supporto del Servizio "Servizi ICT", procederanno alla valutazione della gravità del *Data Breach* occorso. Una copia della valutazione effettuata sarà necessariamente conservata e allegata al Registro dei *Data Breach*.

Qualora dalla valutazione privacy emerga che non ci sono rischi per i diritti e le libertà degli interessati, l'RPD provvederà a classificare l'incidente di GRAVITA' BASSA nell'apposito Registro degli incidenti (all'interno del software GDP) allegando le valutazioni effettuate.

1.7.5 Fase 4: notifica

Se dalla valutazione dovessero invece emergere dei profili di rischio per i diritti e le libertà degli interessati, l'RPD provvederà alla notifica al Garante della Privacy entro 72h dal momento in cui si è venuti a conoscenza del *Data Breach*.

La notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/

L'RPD notificherà la violazione utilizzando strumenti tracciabili e provvedendo ad archiviare tutte le prove dell'avvenuto invio e ricezione dell'atto notificato. Con la notificazione comunicherà altresì il nome e i recapiti del punto di contatto, designato tra i ruoli di riferimento di Ateneo, presso cui ottenere più informazioni sull'accaduto. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 (settantadue) ore, sarà corredata dai motivi del ritardo esposti e dettagliati.

Alla luce delle verifiche effettuate l'RPD, a seguito di valutazione coordinata con il Titolare del trattamento comunicherà agli interessati coinvolti la violazione dei loro dati personali, con modalità tracciabili di corrispondenza, senza ingiustificato ritardo, ma solo nei casi in cui:

b) la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
c) non siano state messe in atto (ovvero non erano applicate ai dati personali oggetto della violazione), prima dell'Incidente, adeguate misure tecniche e organizzative di protezione, tali da rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (a titolo esemplificativo, la crittografia dei dati);
d) successivamente all'Incidente, non siano state adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.

Nei casi in cui detta comunicazione richiederebbe sforzi sproporzionati, si procederà ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati saranno informati allo stesso modo e con riguardo al medesimo contenuto.

L'RPD compilerà a questo punto il Registro dei *Data Breach (all'interno del software GDP)* allegando la valutazione, il modulo di notifica al Garante e, in caso, l'eventuale copia della comunicazione inviata agli interessati.

1.7.6 Fase 5: Training e formazione dei soggetti autorizzati

Dall'analisi e dalla valutazione di un evento, indipendentemente dal fatto che risulti classificabile come incidente trascurabile o ***Personal Data Breach***, possono emergere

- *esigenze di miglioramento delle misure di prevenzione o di sicurezza adottate*: il Servizio "Servizi ICT" provvederà ad informare il management delle azioni ritenute necessarie.
- *esigenze di formazione del personale su eventuali rischi o su modalità di intervento appropriate*: l'RPD informa il Titolare del trattamento dell'esigenza formativa individuata al fine di integrare e aggiornare il piano di formazione di Ateneo.

1.8 CLASSIFICAZIONE DEGLI INCIDENTI:

LIVELLO	STIMA DELLA GRAVITÀ DELL'INCIDENTE O DELLA VIOLAZIONE	DESCRIZIONE	COMUNICAZIONE ALL'AUTORITÀ	COMUNICAZIONE AI SOGGETTI INTERESSATI
0	FALSO ALLARME	Dall'analisi dell'accaduto si rileva un falso allarme, in quanto l'evento è stato erroneamente segnalato come incidente, ma non si qualifica come tale. Si riporta in ogni caso traccia di tale riscontro. Non sono stati prodotti effetti ne rischi sui diritti e libertà delle persone.	NON PREVISTA	NON PREVISTA
1	RISCHIO TRASCURABILE	Dall'analisi dell'accaduto si rilevano situazioni, meglio descritte nel registro degli incidenti, che non producono, ne hanno prodotto effetti o rischi sui diritti e libertà delle persone, oppure è molto improbabile che ne possano produrre. A titolo esemplificativo: a. è stato rubato un computer portatile dotato di doppia autenticazione, il cui hard disk è crittografato; b. l'antivirus ha segnalato un evento, ma automaticamente è stato rimosso o risolto senza ritardo.	NON PREVISTA	NON PREVISTA
2	BASSO RISCHIO	Dall'analisi dell'accaduto si rilevano situazioni, meglio descritte nel registro degli incidenti, che configurano una violazione di dati personali, i cui effetti producono un rischio sui diritti e libertà delle persone valutato come "rischio basso".	SI	SI VALUTA SE NECESSARIO
3	MEDIO RISCHIO	Dall'analisi dell'accaduto si rilevano situazioni, meglio descritte nel registro degli incidenti, che configurano una violazione di dati personali, i cui effetti producono un rischio sui diritti e libertà delle persone valutato come "rischio medio".	SI	SI VALUTA SE NECESSARIO
4	ALTO RISCHIO	Dall'analisi dell'accaduto si rilevano situazioni, meglio descritte nel registro degli incidenti, che configurano una violazione di dati personali, i cui effetti producono un rischio sui diritti e libertà delle persone valutato come "rischio alto".	SI	SI - VALUTARE LA COMUNICAZIONE AGLI ORGANI DI STAMPA

Nella tabella "**Classificazione degli incidenti**":

1. Vengono riportati gli incidenti di sicurezza gestiti che sono qualificati in:
   - 0=falso allarme - 1=rischio trascurabile - 2=basso rischio - 3=medio rischio - 4=alto rischio)
2. A seguito della identificazione o meno della condizione di (2) "basso rischio", o (3) "medio rischio", o (4) "alto rischio" sulla base della valutazione dei soggetti preposti alla valutazione, vengono effettuate le azioni, e se del caso comunicazioni previste secondo gli schemi individuati dai Provvedimenti del 30/07/2019 e del 27/05/2021 del Garante della Privacy.

1.9 CHE TIPO DI VIOLAZIONI DI DATI PERSONALI VANNO NOTIFICATE?

Vanno notificate unicamente le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali.

Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro **significativo svantaggio economico o sociale.**

1.10 CHE INFORMAZIONI DEVE CONTENERE LA NOTIFICA AL GARANTE?

La notifica deve contenere le informazioni previste dall'art. 33, par. 3 del Regolamento (UE) 2016/679 e specificate, secondo la nuova procedura introdotta dal **Provvedimento del Garante n. 209 del 27 maggio 2021**, nel Modello della notifica data breach a ciò destinato disponibile sul sito del Garante al link: **https://servizi.gpdp.it/databreach/s/**.

1.11 COME INVIARE LA NOTIFICA AL GARANTE?

Secondo quanto previsto nel **Provvedimento del Garante n. 209 del 27 maggio 2021**, la notifica deve essere inviata al Garante secondo le modalità riportate sul sito del Garante al link: (https://servizi.gpdp.it/databreach/s/), con preciso riguardo alle indicazioni pratiche e alla descrizione delle funzionalità e dei flussi della nuova procedura telematica.

1.12 LE AZIONI DEL GARANTE

Il Garante può prescrivere misure correttive (v. art. 58, paragrafo 2, del Regolamento UE 2016/679) nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare **fino a 10 milioni di Euro** o, nel caso di imprese, **fino al 2% del fatturato totale annuo mondiale**.

1.13 PROCEDURA DELL'ORGANIZZAZIONE PER LA COMUNICAZIONE DI DATA BREACH

1.13.1 Notifica di *Data Breach* al Garante della Privacy - Art. 33 p.3 GDPR – Art. 26 D.Lgs. 51/2018

Secondo la nuova procedura introdotta dal **Provvedimento del Garante n. 209 del 27 maggio 2021**, una persona fisica - identificata - potrà effettuare la notifica in nome e per conto del titolare del trattamento previa assunzione della responsabilità, ai sensi dell'art. 168 del Codice o dell'art. 44 del Decreto, e del contenuto della stessa, utilizzando obbligatoriamente la funzionalità preposta e il Modello della notifica data breach a ciò destinato disponibili entrambi sul sito del Garante al link: (https://servizi.gpdp.it/databreach/s/)..

1.13.2 Comunicazione di Data Breach ai soggetti interessati - Art. 34 p.2 GDPR – Art. 26 D.Lgs. 51/2018

a) Descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali.

b) Comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.

c) Descrivere le probabili conseguenze della violazione dei dati personali.

d) Descrivere le misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

La comunicazione dovrebbe essere data direttamente e personalmente agli interessati coinvolti dalla violazione, a meno che ciò comporti sforzi sproporzionati. In tal caso, si procede invece ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con la medesima efficacia.

La comunicazione deve essere distinguibile rispetto altre diverse comunicazioni che vengono fatte dal titolare agli interessati, in altri termini, la comunicazione deve essere chiara, inequivocabile e richiamare l'attenzione dell'interessato.

Il rispetto di questi requisiti richiede che il titolare, già prima che si verifichi una causa di comunicazione, considerati i dati che tratta e le categorie di interessati, predisponga un piano specifico di comunicazione.

La comunicazione, pur sussistendo la condizione di rischio elevato, si ritiene soddisfatta quando:

a) il titolare del trattamento ha messo in atto le 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, quali la cifratura;

b) 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.
Mentre per far scattare l'obbligo di notifica è sufficiente che sussista una violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche, per la comunicazione occorre che tale rischio sia elevato.

Il titolare è dunque tenuto non solo ad individuare e qualificare i rischi connessi a violazioni di dati personali, ma, qualora tali rischi riguardino i diritti e le libertà delle persone fisiche, deve anche procedere ad una valutazione del livello di rischio.
Il considerando 76 del GDPR chiarisce che la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

1.14 LINEE GUIDA APPLICABILI

- Linee guida in materia di notifica delle violazioni di dati personali (*Data Breach Notification*) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679, adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017

- Versione emendata e adottata il 6 febbraio 2018;

- Provvedimento del Garante della Privacy italiano del 30 luglio 2019;

- Provvedimento del Garante della Privacy italiano del 27 maggio 2021.