UNIVERSITÀ
DEL SALENTO

# Linee guida e procedura operativa per la gestione degli incidenti sulla sicurezza in ordine ai dati personali (Data Breach) dell'Università del Salento

La realizzazione del documento è stata curata da:

- *Dott.ssa Giuseppina CAMPANILE*
- *Dott.ssa Alessandra CARITÀ*
- *Avv. Maria Ida Anna GIANNELLI*
- *Ing. Tiziana MONTANARO*

# SOMMARIO

# INTRODUZIONE

Il presente documento è stato redatto al fine di fornire una guida operativa di Ateneo in tema di gestione degli incidenti sulla sicurezza nonché di Personal Data Breach in applicazione delle prescrizioni introdotte dalla normativa europea in materia di protezione dati personali, ed in particolare dagli articoli 33 e 34 del Regolamento europeo n.2016/679 (RGPD).

Nella redazione delle presenti Linee Guida si è tenuto conto del:

- "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)" - RGPD;
- Decreto Legislativo 10 agosto 2018 n, 101 "Disposizioni per l'adeguamento della Normativa Nazionale alle disposizioni del 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)";
- Decreto legislativo 30 giugno 2003, numero 196, recante il "Codice in materia di protezione dei dati personali", come modificato, da ultimo, dal Decreto-Legge convertito con modificazioni dalla L. 8 agosto 2019, n. 77;
- 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, approvate, in via definitiva, il 6 febbraio 2018;
- Linee Guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2017/679 adottate il 4 aprile 2017 come modificate il 4.10.2017 dal Gruppo di lavoro articolo 29 per la protezione Dati – WP 248;
- Manuale sulla sicurezza nel trattamento dei dati personali adottato da European Union Agency for Network and Information Security (ENISA) nel dicembre 2017;
- "Guidelines for SMEs on the security of personal data processing" adottate da European Union Agency for Network and Information Security (ENISA) nel dicembre 2016;
- D.Lgs. 82/2005 "Codice dell'Amministrazione Digitale (CAD)" come modificato da ultimo con Decreto-Legge 26 ottobre 2019, n. 124;
- Art. 13 del DPCM Decreto Del Presidente Del Consiglio Dei Ministri 24 ottobre 2014 "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese";
- Artt. 331 e 361 del Codice di Procedura Penale;
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) del 30 luglio 2019.

Il presente documento è suscettibile di integrazioni, modifiche e correttivi alla luce dell'evoluzione della normativa di riferimento

# 1. OBIETTIVO E FINALITÀ

Con l'adozione del presente documento denominato "Linee guida e procedura operativa per la gestione degli incidenti sulla sicurezza in ordine ai dati personali (Data Breach)" l'Ateneo si prefigge di:

- tutelare la sicurezza e la riservatezza delle Informazioni Personali di qualsiasi Interessato (studenti, dipendenti, docenti, collaboratori, contraenti, partecipanti a corsi di formazione e a procedure selettive, etc.…);
- fornire immediata risposta agli Incidenti di Sicurezza nonché ai *Personal Data Breach* come di seguito specificati;
- sensibilizzare i soggetti coinvolti dell'Ateneo sulle responsabilità in materia di protezione dei dati personali e sull'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli Incidenti sulla Sicurezza (inclusi i *Personal Data Breach*), definendo ruoli e responsabilità ed assicurando un adeguato flusso comunicativo ed operativo all'interno dell'Ateneo tra gli attori interessati.

# 2. DEFINIZIONI

Ai fini delle presenti Linee Guida si intende per:

- **Informazioni Personali**: I Dati personali, i Dati particolari ivi inclusi i dati biometrici, i Dati relativi alla salute e i Dati giudiziari.
- **Altre Informazioni:** Informazioni differenti dalle informazioni personali
- **Dati Personali:** Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); 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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Quelli più comunemente usati sono il codice fiscale, il numero di partita IVA, la residenza, il numero di telefono, l'indirizzo e-mail.
- **Dati Particolari:** Dati personali idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti politici, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati genetici, biometrici e i dati idonei a rivelare lo stato di salute e la vita sessuale.
- **Dati Inerenti la Salute:** Dati personali relativi alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano Informazioni relative al suo stato di salute.
- **Dati Biometrici:** Dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
- **Dati Giudiziari:** Dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere a), b) c) d), e), f), g), h), i), i)-bis, i)-ter, l), m), n), o), r), s), t), u) del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli art. 60 e 61 del c.p.p.

- **Trattamento:** qualsivoglia operazione o insieme di operazioni compiute con o senza il supporto di processi automatizzati e applicate a dati personali o insieme 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 altro mezzo di messa a disposizione, il raffronto, l'interconnessione, la limitazione, la cancellazione o la distruzione.
- **Comunicazione:** Rivelazione di dati personali a uno o più enti identificati e diversi dal Soggetto Interessato, rappresentante del titolare del trattamento nel territorio statale, responsabile del trattamento e soggetti responsabili dell'elaborazione sotto qualsiasi forma, incluso il rendere disponibili o accessibili tali dati.
- **Diffusione:** Rivelazione dei dati personali a enti non identificati, sotto qualsiasi forma, incluso il rendere disponibili o accessibili tali dati.
- **Garante**: Autorità Garante per la protezione dei dati personali
- **Titolare del Trattamento:** Persona fisica, persona giuridica, pubblica amministrazione, pubblica autorità e qualsiasi altra associazione od organismo che determina, anche insieme ad altro Titolare, le finalità e i mezzi di trattamento dei dati personali, ivi compreso il profilo di sicurezza.
- **Interessato**: Qualsiasi persona fisica a cui si riferiscono i dati personali
- **Responsabile del Trattamento:** persona fisica o giuridica, autorità pubblica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo che tratta dati personali per conto del titolare del trattamento
- **Board Operativo**: gruppo di soggetti incaricato di gestire gli Incidenti di sicurezza e i *Personal Data Breach*. La composizione del Board Operativo è definita dal Rettore.
- **Responsabile della Protezione dei Dati (DPO):** Soggetto individuato dal Titolare del trattamento per le qualità professionali possedute e per la conoscenza specialistica della materia (normativa e prassi), che viene coinvolto ed interessato in tutte le questioni che riguardano la protezione dei dati personali.
- **Incidente sulla Sicurezza:** Violazione della sicurezza che può anche non riguardare le Informazioni Personali.
- **Violazione di Dati o *Personal 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.
- **Registro delle Violazioni dei Dati Personali o Personal Data Breach**: registro in cui sono documentate le violazioni di dati personali subite e sono annotate tutte le informazioni relative alla violazione.

## 3. AMBITO OGGETTIVO DI APPLICAZIONE

La procedura di cui alle presenti Linee Guida si applica a tutte le Informazioni Personali o altre informazioni gestite o comunque trattate dall'Ateneo, siano esse contenute su supporti cartacei, su dispositivi elettronici, accessibili via rete o web o su dispositivi mobili o portatili.

## *4.* TIPOLOGIE DI VIOLAZIONI E DI *PERSONAL DATA BREACH*

Le violazioni possono essere classificate in:

- "V*iolazione della riservatezza*", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "*Violazione dell'integrità*", in caso di modifica non autorizzata o accidentale dei dati personali;
- "*Violazione della disponibilità*", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Laddove gli incidenti interessino uno dei predetti attributi le violazioni vengono classificate in:

- *"Personal Data Breach sulla Riservatezza"*: violazione della riservatezza delle Informazioni Personali (a titolo esemplificativo: quando si verifica una comunicazione non dovuta o un accesso non autorizzato o accidentale ai dati personali);
- *"Personal Data Breach sull'Integrità"*: quando si verifica una alterazione/modifica non autorizzata o accidentale dei dati personali.
- *"Personal Data Breach sulla Disponibilità"*: quando i dati personali non sono disponibili perché si verifica una loro perdita accidentale o una distruzione (a titolo esemplificativo viene smarrita la chiave di decriptazione dell'unica copia di dati criptati e non è disponibile una copia di backup). La perdita di disponibilità può anche essere temporanea (e configurare, comunque, un Personal Data Breach), vista l'importanza di avere informazioni disponibili in un dato momento.

# 5. PROCEDURE A TUTELA DELLA SICUREZZA DEI DATI – NORME DI CARATTERE GENERALE

## 5.1.Misure Preventive

A tutela della sicurezza dei dati l'Ateno adotta le seguenti misure preventive:

- Predispone azioni e misure sia organizzative che tecniche per assicurare un livello di sicurezza adeguato al rischio connesso al trattamento dei dati personali e alle altre informazioni trattate, comprese misure volte al tempestivo ripristino della disponibilità in caso di Incidente sulla sicurezza;
- Organizza, a cadenza periodica, corsi di formazione per i dipendenti/collaboratori in materia di trattamento dati e di sicurezza dei Dati Personali e dei Sistemi;
- Predispone un sistema di protezione, mediante apposite misure tecniche (*firewall*, *antivirus*…) dell'accesso a Internet e ai dispositivi elettronici.

## 5.2. Comunicazione dell'incidente di sicurezza

Il personale interno ed esterno all'Ateneo che viene a conoscenza, anche a seguito di segnalazione di terzi, di un Incidente sulla sicurezza o di elementi e circostanze che fanno sospettare che si sia verificato o possa verificarsi un incidente, è tenuto a comunicare immediatamente tale circostanza **al Board Operativo e al DPO.**

## 5.3.Risposta all'incidente di sicurezza

La risposta a un Incidente sulla sicurezza o a un *Personal Data Breach* deve avvenire secondo le fasi procedurali descritte nel proseguo.

Le procedure potrebbero, tuttavia, sovrapporsi o richiedere tempistiche differenti o aggiornamenti in ragione della molteplicità delle cause che hanno determinato l'incidente, dei diversi soggetti coinvolti e dei livelli e dell'intensità della gravità delle sue conseguenze.

È dovere prioritario di ciascun soggetto, nell'ambito del proprio ruolo nella struttura e nella catena di comunicazione, considerate le ridotte tempistiche (oggetto di trattazione nel successivo punto 8) per effettuare la Notifica e per la comunicazione agli interessati, occuparsi degli Incidenti di sicurezza, non ritardare, senza giustificato motivo, iniziative di reazione all'incidente e rispettare le procedure e le tempistiche di comunicazione individuate dalle presenti Linee Guida.

La gestione degli Incidenti di sicurezza e dei *Personal Data Breach* deve avvenire garantendo il massimo livello di riservatezza: le informazioni devono essere condivise esclusivamente con il personale identificato nella presente procedura. Con riferimento ai soggetti non coinvolti le eventuali comunicazioni sull'incidente dovranno limitarsi all'indicazione generica che si è verificato un problema e che lo stesso è in fase di gestione.

# 6. VALUTAZIONE PRELIMINARE E GESTIONE DELL'INCIDENTE

## 6.1. Rilevazione dell'Incidente

Qualora si sia verificato un Incidente di sicurezza o si abbia il sospetto che un incidente si possa verificare, le azioni da intraprendere sono le seguenti:

- deve essere effettuata la segnalazione dell'evento, utilizzando le vie più brevi (telefono o via e-mail ai recapiti disponibili sul sito istituzionale – pagina privacy https://www.unisalento.it/privacy), al **Board Operativo** e al **DPO** per gli approfondimenti necessari finalizzati all'identificazione della natura dell'incidente;
- il **Board Operativo informa** dell'evento il Responsabile della Struttura coinvolta nel trattamento dei dati violati mediante l'utilizzo della modulistica disponibile sulla predetta pagina privacy o comunque con altri mezzi ritenuti opportuni purché in forma scritta e provvede all'annotazione sul registro assegnando un numero di riferimento ed inserendo tutte le informazioni in suo possesso come dettagliatamente individuate nel paragrafo 9;
- laddove il **DPO** ritenga che la segnalazione possa riguardare un *Personal Data Beach* in accordo con il Board Operativo informa il Titolare del Trattamento sull'incidente e sugli esiti dell'analisi preliminare svolta;
- il **Board Operativo**, d'intesa con il DPO, avvia azioni tempestive per la risoluzione del problema e, in caso di *Data Breach* informatico, in collaborazione con il **responsabile dell'applicativo IT,** coordina le fasi di valutazione e risoluzione, di seguito definite, compresa l'organizzazione di riunioni, comunicazioni interne, relazioni sulle informazioni raccolte e informative e su ogni altra misura adottata per la gestione dell'Incidente sulla sicurezza. In particolare il **Board Operativo** dovrà immediatamente avviare le necessarie verifiche al fine di appurare se si sia effettivamente verificato un Incidente di sicurezza, accertandone la probabilità e la gravità.

## 6.2. Valutazione preliminare e contenimento dell'incidente

Il **Board Operativo**, appena ricevuta la segnalazione, effettua immediatamente una valutazione preliminare, per determinare se si sia effettivamente verificato un incidente sulla sicurezza e se quest'ultimo possa qualificarsi anche come *Personal Data Breach*.

A conclusione della predetta valutazione, l'Ateneo si considera "*venuto a conoscenza*" della violazione e, conseguentemente, da tale momento iniziano a decorrere i termini per la notifica al Garante e la eventuale comunicazione agli interessati.

Rientra tra i compiti del Board **Operativo**:

- ✓ identificare il dispositivo (computer, apparato mobile, sistema di *backup*, apparato di rete, etc.…) colpito, ed altresì la causa, l'entità, la tipologia di dati o di Informazioni personali coinvolte e la sensibilità delle informazioni;
- ✓ verificare la natura dei soggetti coinvolti (es: dipendenti, studenti, docenti etc.) e il loro numero;
- ✓ verificare se i dati e le Informazioni personali non siano più disponibili ovvero siano comunque accessibili e utilizzabili dall'Ateneo;
- ✓ verificare e stabilire la sussistenza dell'elemento psicologico nella causazione della violazione ovvero se la stessa sia stata intenzionale, colposa o accidentale;
- ✓ valutare le conseguenze della violazione in termini di danni agli Interessati;
- ✓ individuare eventuali azioni che permettano di trattare, eliminare e/o limitare il rischio.

Il Responsabile della protezione (DPO) opportunamente supportato dal **Board Operativo** valuta, secondo i parametri stabiliti nel presente documento, il livello di rischio per gli Interessati (basso, medio, alto o molto alto) di pregiudizio e/o lesione dei diritti e delle libertà fondamentali derivante dall'infrazione.

### 6.3. Comunicazione dei risultati della valutazione preliminare

Il **DPO** informa, ove possibile, entro le 24 ore, il Direttore Generale e il Rettore dell'evento verificatosi, sulla valutazione svolta sino al predetto momento e sul livello di gravità della violazione. Nel caso in cui sia stato accertato un *Personal Data Breach*, il Rettore, con il parere del Responsabile della protezione dei dati, stabilisce se procedere alla notificazione al Garante e alla comunicazione ai soggetti interessati entro i termini di seguito riportati.

## 7. RISOLUZIONE DELL'INCIDENTE

Il **Board Operativo** è responsabile della risoluzione dell'incidente e del *Personal Data* Breach.

Nello specifico:

- valuta se è necessario l'intervento di risorse esterne;
- intraprende azioni immediate per contenere o prevenire ulteriori danni (limitare l'accesso a documenti o sistemi, mettere fuori servizio sistemi e reti, bloccare una porta o un indirizzo IP internamente o esternamente, etc.). Tali restrizioni rimarranno in essere fino alla risoluzione dell'incidente.
- determina la causa e l'ambito della violazione;
- individua dati, sistemi e dispositivi compromessi;
- provvede alla localizzazione, reperimento e conservazione (ove possibile) di tutti i *log* e *record* elettronici (inclusi *backup*, immagini, *hardware*, etc.) e di videosorveglianza per successive fasi legali, apposizione della firma digitale, la marcatura temporale di tutte le evidenze informatiche disponibili;
- nel caso di sospetta attività criminale, fa le comunicazioni del caso all'Area Legale di Ateneo e le segnalazioni alle autorità competenti, ove previsto, ai sensi e per gli effetti dell'artt. 331 c.p.p.;
- valuta tutte le soluzioni per sostituire o ripristinare risorse e macchinari compromessi, inclusi costi di riparazione o recupero dei beni a livelli di sicurezza accettabili.

Ulteriori attività di risoluzione subordinate al tipo di incidente e di dati compromessi, non descritte nel presente documento, verranno stabilite e gestite dal **Board Operativo.**
Il **DPO** comunica l'incidente e le misure risolutive adottate al Rettore, al Direttore Generale. Il **Board Operativo** e il **DPO** stabiliscono quando chiudere l'incidente; in nessun caso l'accesso ai dati o il ripristino di un sistema compromesso tornerà a una regolare operatività senza previa approvazione del *Board Operativo* e del Rettore, d'intesa con il DPO.
**Il Board Operativo** e il **DPO** individuano le misure di correzione e prevenzione dei problemi futuri, compresi, ove ritenuto opportuno, quelli di revisione dei livelli di sicurezza delle informazioni e dei programmi di formazione; di conduzione di audit sulla sicurezza fisica e tecnica; di revisione delle politiche e procedure di Ateneo; di revisione delle pratiche di selezioni dei dipendenti e di tirocinio; di revisione dei fornitori di servizi.
Tali azioni correttive verranno comunicate ai Responsabili di Struttura (Dirigenti e Direttori di Dipartimento) per gli adempimenti conseguenti. Tali misure saranno annotate anche sul Registro dei Trattamenti.

# 8. COMUNICAZIONE AL GARANTE E AGLI INTERESSATI

## 8.1.Decisioni in merito alla notifica al Garante e alla comunicazione agli Interessati

La decisione in merito alle comunicazioni si fonderà sul livello di rischio riscontrato, come calcolato sulla base degli indici di cui al successivo paragrafo 10, ovvero se il livello di rischio è:

- **Nullo/Basso**: non verrà effettuata la notifica al Garante né la comunicazione ai soggetti interessati. L'incidente/*Personal Data Breach* dovrà essere, comunque, registrato dal **Board Operativo** nell'apposito registro e dovranno essere avviate le necessarie misure/azioni per prevenire eventuali ulteriori incidenti;
- **Medio**, il Rettore e il DPO notificheranno il *Personal Data Breach* al Garante utilizzando il modulo messo a disposizione dallo stesso Garante;
- **Elevato o Molto Elevato**, il Rettore e il DPO comunicheranno il *Personal Data Breach* al Garante utilizzando il modulo messo a disposizione dallo stesso Garante e agli Interessati.

## 8.2.Notifica al Garante

Il Rettore, con il parere del Responsabile della protezione dei dati, provvede alla Notifica al Garante quando non è "*improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*". Tale notifica, deve essere effettuata **senza ingiustificato ritardo e, comunque, entro 72 ore** da quando si è avuto conoscenza del *Personal Data Breach*. Superate le 72 ore, la notifica può ancora essere effettuata purché si fornisca adeguata motivazione del ritardo.

## 8.3.Modalità

La notifica al Garante deve avvenire all'indirizzo di posta elettronica indicato sul sito del Garante, secondo le modalità indicate dallo stesso e utilizzando il modulo predisposto ad hoc dal Garante stesso. Il modulo va compilato con firma digitale e inviato via email o posta elettronica certificata. La reperibilità del modulo deve essere garantita direttamente dalla pagina privacy del portale di Ateneo.
Quando, in funzione della natura del *Personal Data Breach*, a seguito della valutazione preliminare di cui al precedente punto 6.2, pur avendo valutato la sussistenza di un *Personal Data Breach*, non è possibile

fornire le informazioni di cui sopra entro i termini previsti (perché ad esempio, in caso *di cyber attack*, devono essere condotte analisi approfondite per stabilire la natura del *Personal Data Breach* e/o il numero o le categorie dei soggetti coinvolti), il **Rettore**, supportato dal **DPO**, sentito il **Board Operativo**, procede ad una Notifica per Fasi dando adeguata motivazione al Garante di tale tipologia di notifica.
Se a seguito di una prima notifica si dovesse appurare che non si è verificato alcun *Personal Data Breach* il DPO deve dare comunicare di tale circostanza al Garante.

## 8.4.Comunicazione ai soggetti interessati

Quando la violazione è suscettibile di presentare un **rischio elevato** per i diritti e libertà fondamentali dei soggetti interessati il Rettore, con il supporto del DPO, provvede alla comunicazione del *Personal Data Breach* agli stessi interessati.
La comunicazione ai soggetti interessati deve avvenire nel più breve tempo possibile e senza ingiustificato ritardo, onde consentire a questi ultimi di mettere in atto misure atte a limitare i danni. In caso di urgenza si può procedere alla comunicazione agli interessati, anche prima di aver effettuato la notifica al Garante.
Il Rettore, con il supporto del DPO, valuta se contattare il Garante per chiedere suggerimenti sulla necessità di comunicare l'incidente agli interessati e sull'individuazione del messaggio più appropriato da adottare.
La comunicazione all'interessato deve essere effettuata con un linguaggio semplice e chiaro; inoltre deve descrivere la natura della violazione dei dati personali e deve contenere almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del RGPD ovvero:

- una breve descrizione dell'accaduto, data (o date) della violazione e della relativa scoperta e descrizione del tipo di Informazioni Personali che sono state compromesse;
- il nome e i dati di contatto del responsabile della protezione dei dati o dei Responsabili del trattamento dei dati da contattare per ottenere maggiori informazioni;
- una descrizione delle probabili conseguenze e del rischio della violazione e dell'entità del danno;
- indicazione delle azioni che gli Interessati e l'Ateneo dovranno intraprendere per limitare l'entità del danno;
- una descrizione delle misure già adottate dall'Ateneo per porre rimedio al *Personal Data Breach* e per attenuarne i possibili effetti negativi e l'entità del danno nonché quelle che sono state e verranno adottate per evitare eventuali future violazioni.

La comunicazione è individuale ed è compiuta per iscritto (via e-mail, tramite sms, etc.). Il mezzo per effettuare la comunicazione andrà scelto in base al numero dei soggetti interessati da contattare, al costo e ai mezzi normalmente utilizzati per le comunicazioni con i soggetti interessati.

Tuttavia, ove la suddetta comunicazione richiedesse degli sforzi sproporzionati, è possibile procedere anche con una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (es. *banner* o *post* su sito internet, pubblicazione di annuncio sul giornale, etc.).

In ogni caso, la comunicazione deve essere effettuata con strumenti in grado da garantire che gli interessati siano effettivamente informati del fatto che si è verificato un *Personal Data Breach*.

Non è richiesta la comunicazione all'Interessato in una delle seguenti ipotesi:

- se il titolare del trattamento ha già applicato misure tecniche ed organizzative adeguate per proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali ad esempio la cifratura;

- se, immediatamente dopo la violazione, il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio ai diritti e alle libertà delle persone fisiche;
- ove, contattare gli interessati richiedesse uno sforzo sproporzionato, ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti. In tale caso si procede con una comunicazione pubblica o di addotta una misura analoga, tramite la quale gli interessati vengano informati in maniera altrettanto efficace.

# 9. REGISTRO DEL PERSONAL DATA BREACH

È istituito un registro in cui il ***Board Operativo***, per quanto di sua competenza, dovrà documentare gli incidenti di sicurezza/*Personal Data Breach* a prescindere dal fatto che da questi sia seguita la notifica al Garante e/o la comunicazione agli Interessati.

Il registro contiene:

- data e ora della violazione;
- descrizione della violazione dei dati oggetto di violazione;
- fonte dell'informazione sulla violazione;
- cause della violazione;
- effetti e conseguenze della violazione (quantità dei dati personali e degli interessati coinvolti dalla violazione);
- indicazione della notifica della violazione all'Autorità di controllo;
- indicazione della comunicazione al/i soggetto/i interessato/i nell'ipotesi di Personal Data Breach con specificazione dei tempi e degli strumenti di comunicazione utilizzati;
- motivo per il quale la violazione è stata ritardata o non è stata comunicata all'autorità di controllo;
- ragioni che hanno indotto alla Notifica per fasi;
- provvedimenti adottati a seguito della violazione per porvi rimedio.

# 10. CALCOLO DEL LIVELLO DI RISCHIO

## 10.1. Valutazione del rischio

Per calcolare il livello del rischio occorre tener conto della probabilità di accadimento del danno e della gravità delle conseguenze per i diritti e le libertà degli interessati.

Elementi fondamentali della valutazione del rischio sono:

- Il tipo di violazione, ovvero se relativa alla riservatezza, disponibilità o integrità di dati come delineati al punto 4 del presente documento (ad esempio una violazione concernente la confidenzialità dei dati riguardanti la carriera di uno studente può avere un livello di rischio e un impatto diverso - e minore- rispetto alla perdita o distruzione definitiva dei predetti dati);
- Natura, carattere sensibile e volume dei dati personali; più i dati sono sensibili, più il rischio è maggiore. Una combinazione di dati personali ha un carattere più sensibile rispetto ad un solo dato personali (ad esempio la violazione della confidenzialità dei dati sulla salute ha delle conseguenze più gravi della violazione della confidenzialità dei dati anagrafici di un soggetto);

- Facilità d'identificazione degli interessati; l'identificazione può essere direttamente o indirettamente possibile a partire dai dati oggetto di violazione, ma può dipendere anche dal contesto specifico della violazione e dalla disponibilità pubblica dei corrispondenti dettagli personali. Ove l'incidente riguardi dati che non permettono la diretta identificazione degli Interessati, il livello di rischio è minore (ad esempio la violazione di dati criptati o de identificati è sicuramente meno grave della violazione di dati in chiaro o accompagnati dagli identificativi diretti degli Interessati);
- Gravità delle conseguenze per i soggetti interessati: tanto maggiori saranno le conseguenze nell'ipotesi in cui dalla violazione dei dati possa derivare un furto o usurpazione di identità, danni fisici, disagio psicologico, umiliazione o danni alla reputazione. Il livello di rischio è maggiore se il Titolare è a conoscenza che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose.
- Caratteristiche particolari dell'interessato (minori o altre persone fisiche vulnerabili);
- Numero delle persone interessate; maggiore è il numero degli interessati più elevato il rischio.

Ad ogni buon conto la valutazione deve essere svolta sempre in relazione alla fattispecie concreta specifica ed avendo riguardo al contesto di riferimento.

## 10.2. Calcolo del rischio

Il rischio (R) è calcolato con la formula: *R = Probabilità della minaccia x Impatto*

Il rischio è tanto maggiore quanto più è probabile che accada l'incidente e tanto maggiore è la gravità del danno arrecato (impatto).

Una volta attribuiti i valori alle due variabili "Probabilità della Minaccia" e "Impatto", il rischio è numericamente definito con una scala crescente da 1 a 12 come riportato nella seguente tabella

| | LIVELLO DI IMPATTO | | | |
|---|---|---|---|---|
| PROBABILITÀ DELLA MINACCIA | Basso (1) | Medio (2) | Alto (3) | Molto Alto (4) |
| Basso (1) | 1 | 2 | 3 | 4 |
| Medio (2) | 2 | 4 | 6 | 8 |
| Alto (3) | 3 | 6 | 9 | 12 |

## 10.3. Voci del calcolo del rischio: la probabilità e il livello di impatto

**La probabilità** di una minaccia è misurata mediante la ponderazione delle variabili che influenzano il trattamento del dato come: le risorse di rete e le tecniche utilizzate, i processi e le procedure relativi al trattamento dei dati personali, le parti/persone coinvolte nel trattamento dei dati personali e il settore di operatività, la scala/dimensione del trattamento svolto.

A tal fine si fa espresso richiamo alle "*Guidelines for SMEs on the security of personal data processing*" del dicembre 2016, pagg. da 24 a 30, e "*Manuale sulla sicurezza nel trattamento dei dati personali*" del dicembre 2017 pagg. da 10- 19 redatti entrambi da European Union Agency for Network and Information Security (ENISA)

**L'impatto** della violazione viene misurato in base ai soggetti coinvolti nel trattamento e viene classificato in Nullo/basso, Medio, Alto, Molto Alto, che si traduce in:

- **Nullo/Basso**: Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.)
- **Medio**: Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
- **Alto**: Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
- **Molto Alto**: Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

## 11. INOSSERVANZA DELLA PROCEDURA

La violazione di quanto previsto nel presente documento espone il Titolare del trattamento al rischio di responsabilità civile, penale e amministrativa.
L' autore materiale delle violazioni, laddove trattasi di soggetto interno all'Ateneo, potrà incorrere anche in responsabilità disciplinare ed è passibile di sanzioni disciplinari sulla base della normativa vigente in materia e dal CCNL di riferimento applicabile.

Allegati:

1) Modello Registro Data Breach
2) Modello di comunicazione del Data Breach al Garante
3) Diagramma del flusso procedurale