Università Ca'Foscari Venezia

Policy per la gestione degli incidenti sulla sicurezza in ordine ai dati personali (*Data Breach*) all'Università Ca' Foscari Venezia

Scopo/Premessa

L'Università Ca' Foscari Venezia (d'ora in avanti Ca' Foscari o Ateneo) protegge la sicurezza e la riservatezza delle Informazioni Personali di qualsiasi Interessato (studenti, dipendenti, docenti in visita, partecipanti a corsi di formazione, etc…) e fornisce immediata risposta (i) agli Incidenti di Sicurezza (da intendersi come qualsiasi incidente, a prescindere dall'eventuale interessamento di Dati Personali) nonché (ii) ai *Personal Data Breach* (da intendersi come ogni Incidente sulla sicurezza che coinvolge Dati Personali), come di seguito meglio definiti.

Qualsiasi Incidente sulla Sicurezza e qualsiasi *Personal Data Breach*, rilevato dai collaboratori o portato all'attenzione di tutti i collaboratori che operano, a vario titolo, presso Ca' Foscari, deve essere gestito secondo le modalità definite nelle pagine seguenti.

L'obiettivo del presente documento è:

- sensibilizzare i dipendenti 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*);
- definire processi per identificare, tracciare e reagire ad un Incidente sulla Sicurezza e a un *Personal Data Breach*, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di *Personal Data Breach*, si renda necessario procedere alla (i) notifica al Garante e (ii) comunicazione agli Interessati;
- definire ruoli e responsabilità per la risposta agli Incidenti sulla Sicurezza e ai *Personal Data Breach*;
- assicurare un adeguato flusso comunicativo all'interno di Ca' Foscari tra le parti interessate.

A. Definizioni

Altre informazioni	Informazioni diverse dalle Informazioni personali.
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.
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 comuni	Categoria non definita nella normativa. Fanno parte dei dati comuni il codice fiscale, il numero di partita IVA, la residenza, il numero di telefono, l'indirizzo e-mail.
Dati giudiziari	Dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a 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 codice di procedura penale.

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 personali	Qualunque informazione relativa ad una persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (per es. n. di matricola), i dati relativi all'ubicazione, un identificativo on line. Si considera identificabile la persona fisica che può essere identificata anche tramite uno o più elementi della sua identità fisica, psichica, economica, culturale, sociale.
Dati relativi alla salute	Dati personali attinenti 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.
Diffusione	Rivelazione dei dati personali a enti non identificati, sotto qualsiasi forma, incluso il rendere disponibili o accessibili tali dati.
Garante	L'Autorità Garante per la protezione dei dati personali.
Incidente sulla sicurezza	Violazione della sicurezza che può anche non riguardare le Informazioni Personali.
Informazioni Personali	I Dati personali, i Dati comuni, i Dati particolari ivi inclusi i dati biometrici, i Dati relativi alla salute e i Dati giudiziari.
Interessato	Qualsiasi persona fisica a cui si riferiscono i dati personali.
Incident Owner	È il soggetto incaricato di gestire i *Personal Data Breach* e gli Incidenti di sicurezza. L'*Incident Owner* coincide con il responsabile tecnico dell'applicazione o del sistema coinvolto nel caso di incidenti collegati a sistemi informatici, con il Dirigente dell'Area, il Direttore del Dipartimento, il Direttore del Centro interessato dall'incidente in tutti gli altri casi.
Responsabile del trattamento	Persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento dei dati personali.
Responsabile della protezione dei Dati o DPO	Soggetto individuato dal Titolare in funzione delle qualità professionali e della conoscenza specialistica della normativa e della prassi in materia di protezione dati che deve essere necessariamente coinvolta in tutte le questioni che riguardano la protezione dei dati personali.
Titolare del trattamento	Persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo di sicurezza.
Trattamento	Qualsiasi operazione o serie di operazioni eseguite con o senza l'ausilio di mezzi elettronici o automatici che riguarda la raccolta, registrazione, organizzazione, mantenimento, interrogazione, elaborazione, modifica, selezione, recupero, confronto, utilizzo, interconnessione, blocco, comunicazione, divulgazione, cancellazione e distruzione di dati, che questi siano o meno contenuti in una banca dati.
Violazione di dati o *Personal Data Breach*	Violazione della sicurezza che comporta, in modo accidentale o illecito, la distruzione, perdita, alterazione, comunicazione non autorizzata di, o accesso a, dati personali trasmessi, conservati o altrimenti trattati. La violazione dei dati è quindi un incidente di sicurezza che riguarda le Informazioni Personali.

B. Ambito di applicazione

La presente procedura si applica a tutte le Informazioni Personali e alle altre informazioni che, pur non costituendo Informazioni Personali, sono raccolte o gestite o comunque trattate da Ca' Foscari, siano esse dati contenuti su dispositivi elettronici, accessibili via rete o web, contenuti su dispositivi mobili o portatili ovvero su supporti cartacei.

C. Ruoli e tipologie di *Personal Data Breach*

La tempestività è un fattore determinante nella risposta agli Incidenti sulla sicurezza e ai *Personal Data Breach* ed è dovere di ciascun soggetto, nell'ambito del proprio ruolo nella struttura e nella catena di comunicazione, non ritardare iniziative di reazione all'incidente e rispettare le procedure e le tempistiche di comunicazione individuate dal presente documento.

Coerentemente con il concetto di sicurezza (Riservatezza, Disponibilità e Integrità), gli incidenti possono avere per oggetto di uno o più di questi attributi. Laddove interessino uno solo dei sotto indicati attributi, questi vengono classificati in:

1. *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);
2. *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;
3. *Personal Data Breach* sull'Integrità: quando si verifica una alterazione non autorizzata o accidentale dei dati personali.

D. Procedure a tutela della sicurezza dei dati

1) <u>Preparazione</u>

Presso Ca' Foscari sono state attivate procedure a tutela della sicurezza dei dati, tra cui:

- l'adozione di misure organizzative e tecniche per garantire 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;
- l'organizzazione, a cadenza periodica, di corsi di formazione per i dipendenti/collaboratori sui principi cardine della normativa sul trattamento dati, sulla sicurezza dei Dati Personali e dei Sistemi;
- la predisposizione di un sistema di protezione, mediante apposite misure tecniche (*firewall*, *antivirus*,…) dell'accesso a internet e ai dispositivi elettronici.

Il personale e i collaboratori che prestano attività in Ca' Foscari, ove dovessero venire a conoscenza di un Incidente sulla sicurezza o di elementi che fanno sospettare (anche a seguito di segnalazione di terzi) che si sia verificato o possa verificarsi un tale incidente, sono tenuti a comunicare immediatamente tale circostanza all'Ufficio Supporto Utenti dell'Area Sistemi Informativi e Telecomunicazioni (ASIT).

Il pubblico, per segnalare eventuali anomalie o disservizi, potrà contattare l'Ufficio Relazioni con il Pubblico (URP) che, a sua volta, dovrà informare immediatamente l'Ufficio Supporto Utenti.

2) Risposta: norme generali

La risposta a un Incidente sulla sicurezza o a un *Personal Data Breach* deve avvenire secondo le fasi descritte di seguito. Considerando, tuttavia, che gli Incidenti possono avere molteplici cause o coinvolgere diversi soggetti ed avere conseguenze caratterizzate da vari livelli di gravità, tali fasi potrebbero sovrapporsi o richiedere tempistiche differenti o aggiornamenti.

Considerati i rischi e, in caso di *Personal Data Breach*, le ridotte tempistiche per effettuare la Notifica e per la comunicazione agli interessati, **occuparsi degli Incidenti di sicurezza deve essere obiettivo prioritario per tutti i soggetti coinvolti nella loro gestione**.

Tutti gli Incidenti di sicurezza e i *Personal Data Breach* devono essere trattati con il massimo livello di riservatezza: le informazioni devono essere condivise esclusivamente con il personale identificato nella presente procedura e solo quando strettamente necessario. Eventuali comunicazioni a soggetti non coinvolti nella gestione dell'Incidente dovranno limitarsi all'indicazione che si è verificato un problema e che lo stesso è in fase di gestione.

3) Rilevazione

Nel caso in cui si sia verificato un Incidente di sicurezza o si abbia il sospetto di un incidente, le azioni da seguire sono le seguenti:

a) dovrà essere avvertito l'Ufficio Supporto Utenti per gli approfondimenti necessari e per l'identificazione della natura dell'evento. L'operatore dell'Ufficio Supporto Utenti documenta l'evento nel software a sua disposizione, che assegna un numero di riferimento, e inserisce tutte le informazioni in suo possesso quali data, orario, luogo, fonte della segnalazione, sistema ed entità della violazione;

b) l'operatore dell'Ufficio Supporto Utenti contatta immediatamente via email ed anche via telefono l'*Incident* Owner e nel caso di incidenti legati ai sistemi informatici il Dirigente di ASIT;

c) ove, a valle di una prima analisi, l'*Incident Owner* ritenga che si sia verificato un *Personal Data Breach* contatta immediatamente il Responsabile della protezione dei dati (DPO);

d) l'*Incident Owner* è incaricato di intraprendere delle azioni tempestive per risolvere il problema. In caso di sua assenza, nel caso di *Data Breach* informatici, il Dirigente ASIT può incaricare un altro amministratore di sistema, in caso di *Data Breach* cartacei, il Rettore potrà incaricare un altro soggetto;

e) l'*Incident Owner* gestisce, in caso di *Data Breach* informatico in collaborazione con il Dirigente ASIT, e coordina le fasi di valutazione e risoluzione, di seguito definite, compresa l'organizzazione di riunioni, comunicazioni interne, relazioni sulle informazioni raccolte e informative su ogni altra misura intrapresa per la gestione dell'Incidente sulla sicurezza. In particolare, l'*Incident Owner* dovrà immediatamente avviare le necessarie verifiche al fine di appurare se si sia effettivamente verificato un Incidente di sicurezza, valutandone la probabilità e gravità. L'*Incident Owner* può incaricare un soggetto esterno qualificato per avere conferma della sussistenza di un Incidente di sicurezza.

4) Valutazione e contenimento

Valutazione Preliminare

L'*Incident Owner* effettua immediatamente una valutazione preliminare, al fine di determinare se si sia effettivamente verificato un incidente sulla sicurezza e determina, inoltre, se quest'ultimo possa qualificarsi anche come *Personal Data Breach*. Al termine di tale valutazione preliminare, l'Ateneo si

considera "venuto a conoscenza" della violazione e, conseguentemente, da tale momento inizieranno a decorrere i termini per la notifica e la comunicazione.

A tal fine, l'*Incident Owner* dovrà, per quanto possibile:

- identificare il dispositivo (computer, apparato di rete, apparato mobile, sistema di *backup*, etc...) colpito, nonché 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) e il loro numero;
- verificare se i dati e le Informazioni personali non siano più disponibili ovvero rimangano comunque accessibili e utilizzabili dall'Ateneo;
- stabilire se l'infrazione sia stata intenzionale, colposa o accidentale;
- valutare se l'incidente possa causare danni agli Interessati e determinare la probabilità e gravità del danno;
- individuare eventuali misure che permettano di trattare il rischio.

Inoltre, l'*Incident Owner*, in caso di *Personal Data Breach*, opportunamente supportato dal Responsabile della protezione dei dati, valuta, secondo i criteri stabiliti nelle tabelle di cui al paragrafo VII, il livello di rischio per gli Interessati (basso, medio, alto o molto alto) di pregiudizio/lesione dei diritti e alle libertà fondamentali derivante dalla violazione.

Comunicazione dei risultati dell'*assessment*

L'*Incident Owner* informa, ove possibile, entro le 24 ore, il Direttore Generale e il Rettore sull'evento, sui progressi della valutazione e sul livello di gravità della violazione. Nel caso di *Personal Data Breach* conclamato, 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 sotto indicati.

Decisioni in merito alla notifica al Garante e alla comunicazione agli Interessati

La decisione sarà basata sul livello di rischio secondo quanto segue. 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 dall'*Incident Owner* nell'apposito registro di cui al paragrafo E e dovranno essere avviate le necessarie contromisure per prevenire eventuali ulteriori incidenti;
- **Medio, Elevato o Molto elevato**, il Rettore notificherà il *Personal Data Breach* al Garante;
- **Elevato o Molto elevato**, il Rettore comunicherà il *Personal Data Breach* agli Interessati secondo quanto indicato al paragrafo D.

L'*Incident Owner* intraprenderà azioni immediate per contenere o prevenire ulteriori danni, quali, ad esempio, limitare l'accesso a documenti o sistemi, mettere fuori servizio sistemi e reti, bloccare una porta o un indirizzo IP internamente o esternamente. Tali restrizioni rimarranno in essere fino alla risoluzione dell'incidente.

5) Risoluzione

L'*Incident Owner* è responsabile della risoluzione dell'incidente e del *Personal Data Breach* e stabilisce se è necessario l'intervento di risorse esterne. Le fasi di risoluzione comprendono:

- determinazione della causa e dell'ambito;
- individuazione dei dati, sistemi e dispositivi compromessi;
- gestione o attenuazione della causa della violazione;

- 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; l'apposizione della firma digitale e la marcatura temporale di tutte le evidenze informatiche disponibili;
- nel caso di sospetta attività criminale, comunicazione ai consulenti legali e segnalazione alle autorità competenti, ove previsto;
- valutazione di tutte le alternative per sostituire o ripristinare risorse e macchinari compromessi, inclusi costi di riparazione o ripristino dei beni a livelli di sicurezza accettabili;
- in nessun caso l'accesso ai dati o il ripristino di un sistema compromesso tornerà a una regolare operatività senza previa approvazione dell'*Incident Owner*, del Dirigente ASIT e del Rettore.

Ulteriori attività di risoluzione subordinate al tipo di incidente e di dati compromessi, non descritte nel presente documento, verranno stabilite e gestite dall'*Incident Owner*.

L'*Incident Owner* comunica l'incidente e le misure risolutive adottate al Rettore, al Direttore Generale e nel solo caso di *Data Breach* informatici al Dirigente ASIT. L'*Incident Owner* e i citati soggetti stabiliscono quando ritenere l'incidente risolto e, quindi, chiuso. Sarà l'*Incident Owner* a comunicare all'Ufficio Supporto Utenti di chiudere l'incidente.

L'*Incident Owner* gestisce le azioni correttive per prevenire problemi futuri, compresi:

- revisione dei livelli di sicurezza delle informazioni e dei programmi di formazione;
- conduzione di audit sulla sicurezza fisica e tecnica;
- revisione delle politiche e procedure di Ateneo;
- revisione delle pratiche di selezioni dei dipendenti e di tirocinio;
- revisione dei fornitori di servizi.

6) Comunicazione all'esterno: notifica al Garante e comunicazione agli Interessati

Notifica al Garante

Il Rettore, con il supporto 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 valutazione dovrà essere effettuata utilizzando le tabelle riportate al paragrafo E.

Il Rettore, con il supporto del Responsabile della Protezione Dati, notifica il *Personal Data Breach* al Garante, **senza ingiustificato ritardo e, ove possibile, entro 72 ore** da quando si è avuto conoscenza del *Personal Data Breach*, utilizzando il modulo messo a disposizione dal Garante. Il modulo va compilato con firma digitale e inviato via email o posta elettronica certificata all'indirizzo che messo a disposizione dal Garante.

Quando, in funzione della natura del *Personal Data Breach*, a seguito dell'*assessment* preliminare di cui al precedente punto 4, pur avendo valutato la sussistenza di un *Personal Data Breach*, non è possibile fornire le informazioni di cui ai moduli sopra indicati 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, con il supporto del Responsabile della protezione dati, sentito l'*Incident Owner* e il Dirigente ASIT, procede ad una notifica parziale. Quest'ultima dovrà essere successivamente integrata senza ingiustificato ritardo (notifica per fasi). In questo caso, senza ingiustificato ritardo e, ove possibile, entro 72 ore da quando si è avuto conoscenza del *Personal Data Breach*, dovrà essere notificato al Garante che si è verificato un possibile *Personal Data Breach*, precisando che verranno successivamente fornite maggiori informazioni. Dovranno essere anche fornite le ragioni per cui si ricorre alla Notifica per fasi.

Il Rettore, avvalendosi del supporto del Responsabile della protezione dati, ove a seguito di una prima notifica dovesse appurare che in realtà non si è verificato alcun *Personal Data Breach* deve comunicare tale circostanza al Garante.

Comunicazione ai Soggetti Interessati

Il Rettore, con il supporto del Responsabile della protezione dei dati, provvede alla comunicazione ai soggetti interessati dal *Personal Data Breach* quando la violazione è suscettibile di presentare un **rischio elevato** per i loro diritti e libertà fondamentali. Anche tale valutazione dovrà essere effettuata utilizzando le tabelle riportate al paragrafo E.

La comunicazione ai soggetti interessati deve avvenire nel più breve tempo possibile e senza ingiustificato ritardo, al fine di permettere a questi ultimi di adottare le necessarie contromisure per limitare i danni. In caso di urgenza, si può rendere necessario procedere alla comunicazione agli Interessati anche prima di aver effettuato la notifica al Garante.

Il Rettore, avvalendosi del supporto del Responsabile della Protezione dei Dati, valuta se contattare il Garante per chiedere suggerimenti sulla necessità di comunicare l'incidente agli interessati e sull'individuazione del messaggio più appropriato da fornire.

Lo strumento per effettuare tale comunicazione varia in base al numero dei soggetti interessati da contattare, al costo e ai mezzi normalmente utilizzati per le comunicazioni con i soggetti interessati.

La comunicazione è individuale e compiuta per iscritto (via e-mail, tramite sms, etc...). Tuttavia, ove ciò richiedesse degli sforzi sproporzionati, è possibile procedere anche con una comunicazione pubblica (*banner* o *post* su sito internet, pubblicazione di annuncio sul giornale, etc...). In ogni caso, la comunicazione deve essere trasparente ed effettuata con mezzi tali da garantire che gli interessati siano effettivamente informati del fatto che si è verificato un *Personal Data Breach*.

La comunicazione dovrà contenere:

- 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;
- potenziale rischio causato dalla violazione e entità del danno;
- azioni che gli Interessati e l'Ateneo dovranno intraprendere per limitare l'entità del danno;
- la descrizione delle misure già adottate dall'Ateneo per porre rimedio al *Personal Data Breach* e per attenuarne le conseguenze nonché quelle che sono state e verranno adottate per evitare eventuali future violazioni;
- il nominativo e i recapiti (numero di telefono, indirizzi e-mail) del Responsabile della protezione dei dati o dei Responsabili del trattamento dei dati da contattare per ottenere maggiori informazioni.

Non è richiesta la comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

- il Titolare del trattamento ha messo in atto misure di sicurezza tecniche e organizzative adeguate e tali misure sono state applicate ai dati personali oggetto della violazione. In particolare, rilevano le misure di sicurezza che rendono i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali per esempio la cifratura;
- il Titolare del trattamento ha adottato successivamente all'incidente misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece alla pubblicazione di un avviso pubblico o all'adozione di altre misure simili, tramite le quali gli interessati sono informati con analoga efficacia.

E. Registro dei *Personal Data Breach*

È istituito un registro in cui gli *Incident Owner*, per quanto di loro competenza, dovranno 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 deve contenere (i) la descrizione della tipologia di dati oggetto della violazione, (ii) le cause, (iii) gli effetti, (iv) le azioni poste in essere per rimediarvi, (v) le motivazioni per le quali si è deciso di non procedere alla notifica al Garante e/o alla comunicazione agli Interessati ovvero l'indicazione della notifica effettuata e delle eventuali successive integrazioni.

Dovranno essere altresì documentate le ragioni che hanno condotto alla Notifica per fasi o al ritardo nella notifica.

Il registro dovrà inoltre indicare se, a seguito di un *Personal Data Breach*, è stata effettuata la comunicazione al soggetto interessato, i relativi tempi e mezzi di comunicazione utilizzati.

Il registro è tenuto dal Dirigente di ASIT e viene compilato sulla base delle indicazioni ottenute degli *Incident Owner*.

F. Calcolo del livello di rischio

Per effettuare la predetta valutazione, vengono utilizzati i criteri di seguito elencati, tenendo conto della probabilità di accadimento del danno e della gravità delle conseguenze. Tali criteri rappresentano una mera esemplificazione, fermo restando che la valutazione andrà condotta sul caso specifico e con riguardo al contesto di riferimento.

Tipologia di *Data Breach*	Si dovrà valutare se il *Data Breach* è relativo alla confidenzialità, disponibilità e/o integrità dei dati. Si consideri che 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, tipologia e sensibilità dei dati violati	Generalmente, maggiore è la sensibilità dei dati violati maggiore è il rischio di lesione dei diritti e delle libertà degli individui (per 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 diretta o indiretta dei soggetti interessati	Ove l'incidente riguardi dati che non permettono la diretta identificazione degli Interessati, il livello di rischio è minore (per es. 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	Ad esempio, il rischio dovrà essere valutato elevato ove dalla violazione possa derivare un furto di identità, un danno materiale, un danno di immagine. Analogamente, deve considerarsi elevato il rischio qualora siano stati violati i diritti e le libertà fondamentali dei soggetti interessati quando il Titolare è consapevole che i dati personali sono stati violati e si ritiene che il soggetto che li detiene abbia intenzioni sospette o malevoli.
Categorie dei soggetti interessati	In caso di violazione di Informazioni Personali concernenti minori o soggetti vulnerabili (ad esempio soggetti con disabilità etc...) il rischio si considera più elevato.
Numero di soggetti coinvolti	Generalmente, maggiore è il numero di soggetti interessati, più elevato è il rischio.

Il rischio (R) è calcolato mediante la seguente 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 determinati gli indici di rischio sarà possibile individuarne la significatività e definire quindi le priorità d'intervento. In base ai valori attribuibili alle due variabili "Probabilità della Minaccia" e "Impatto", il rischio è numericamente definito con una scala crescente dal valore 1 al valore 12 secondo la matrice riportata nella seguente tabella

	IMPATTO			
PROBABILITÀ DELLA MINACCIA	Basso (1)	Medio (2)	Elevato (3)	Molto Elevato (4)
Basso (1)	1	2	3	4
Medio (2)	2	4	6	8
Alto (3)	3	6	9	12

La probabilità è misurata mediante la ponderazione delle variabili che influenzano il trattamento del dato come: le risorse tecniche utilizzate, i processi e le procedure e la tipologia di trattamento svolto. Per maggiori dettagli si rinvia al documento dell'ENISA denominato "*Guidelines for SMEs on the security of personal data processing*" del dicembre 2016, pagg. da 24 a 30.

L'impatto della violazione viene misurato in base ai soggetti coinvolti nel trattamento.

LIVELLI DI IMPATTO	
Nullo/Basso	I soggetti interessati non vengono colpiti o subirebbero disagi minimi, superabili senza alcun problema (tempo necessario per reinserire le informazioni, fastidio, irritazione etc…)
Medio	I soggetti interessati subiscono notevoli disagi risolvibili con qualche difficoltà (costi extra, negazione accesso a servizi aziendali, timori, difficoltà di comprensione, stress, indisposizione fisica, etc...)
Elevato	I soggetti interessati subiscono notevoli disagi risolvibili con serie difficoltà (appropriazione indebita di fondi, inserimento nella *black list* dei cattivi pagatori da parte delle banche, danni a proprietà, perdita dell'impiego, citazione a comparire, peggioramento dello stato di salute, etc…)
Molto Elevato	I soggetti interessati subiscono notevoli conseguenze, perfino irreversibili, e impossibili da risolvere (difficoltà finanziarie quali ingenti debiti, impossibilità a lavorare, problemi fisici o psicologici a lungo termine, morte, etc...)

G. Violazioni della presente procedura

La violazione di quanto previsto nella presente *Policy* espone il Titolare del trattamento al rischio di responsabilità civile, penale e a sanzioni amministrative. Il soggetto autore delle violazioni potrà incorrere in responsabilità disciplinare e conseguentemente nei provvedimenti sanzionatori, secondo quanto previsto dalla normativa vigente e dal CCNL di riferimento applicabile.

Allegato: esempi di *Data Breach* e comunicazioni

Caso	Notificare l'autorità di controllo?	Notificare la persona interessata?	Note/raccomandazioni
Un titolare del trattamento ha memorizzato un backup di archivio dati personali criptati su una chiavetta USB. La chiavetta UBS viene rubata durante un furto con scasso.	No.	No.	Fintanto che i dati sono criptati con un algoritmo di ultima generazione, che esistono dei *backup* dei dati che possono essere recuperati in tempi rapidi, e che la chiave univoca non sia stata compromessa, non si tratta di una violazione da notificare. Tuttavia, se successivamente compromessa, la violazione va notificata.
Un titolare del trattamento offre un servizio online. Durante un attacco informatico a tale servizio vengono prelevati dei dati personali di individui. Il titolare del trattamento ha clienti in un singolo Stato membro.	Sì. Notificare l'autorità di controllo competente in presenza di potenziali conseguenze per singoli individui.	Sì. Notificare gli individui a seconda della natura dei dati personali interessati, e nel caso in cui vi siano alte potenziali conseguenze per gli individui.	Se il rischio non è elevato, è consigliabile che il titolare del trattamento informi la persona interessata, a seconda delle circostanze del caso. Potrebbe ad esempio non essere necessario informare nel caso di violazione di una newsletter relativa a un programma televisivo, tuttavia la notifica potrebbe essere necessaria se la newsletter può influenzare il punto di vista politico sull'argomento trattato.
Una breve interruzione di corrente elettrica della durata di qualche minuto presso il call center del titolare del trattamento non ha consentito ai clienti né di chiamare il titolare del trattamento né di accedere ai propri archivi.	No.	No.	Non si tratta di una violazione di dati personali notificabile, sebbene si tratti comunque di un incidente registrabile ai sensi dell'articolo 33. Il titolare del trattamento deve assicurare la registrazione del caso.

Caso	Notificare l'autorità di controllo?	Notificare la persona interessata?	Note/raccomandazioni
Un titolare del trattamento viene fatto oggetto di un attacco con richiesta di riscatto in seguito al quale tutti i dati vengono criptati. Non sono disponibili *backup* e non è possibile ripristinare i dati. In seguito ad accertamenti emerge con certezza che l'unico scopo dell'attacco era quello di criptare i dati, e che non vi è alcun altro *malware* presente nel sistema.	Sì. Notificare l'autorità di controllo competente se vi sono potenziali conseguenze per le persone poiché ciò rappresenta una mancanza di disponibilità.	Sì. Notificare i soggetti a seconda della natura dei dati personali interessati, del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	Nel caso vi sia un *backup* disponibile e i dati possano essere ripristinati in breve tempo, non è necessario segnalare l'evento all'autorità di controllo o alle persone, in quanto non vi si configura una mancanza permanente di disponibilità né di riservatezza. Tuttavia, le autorità di controllo potrebbe ritenere necessaria un'indagine per valutare la conformità con i requisiti di sicurezza generali di cui all'art. 32.
Una persona chiama il call center di una banca segnalando una violazione di dati. Questo individuo ha ricevuto l'estratto conto mensile di qualcun altro. Il titolare del trattamento svolge una breve indagine (entro le 24 ore) e stabilisce con ragionevole certezza che vi è stata una violazione di dati personali, e se si tratti di un difetto sistemico che potrebbe compromettere anche altri soggetti.	Si.	Vanno notificate soltanto le persone interessate, se vi è un alto rischio e se risulta evidente che non siano stati coinvolti altri.	Se in seguito a ulteriori indagini emerge che sono interessati anche altri individui, è necessario un aggiornamento all'autorità di controllo e il titolare del trattamento dovrà notificare altri soggetti nel caso in cui vi sia per essi un rischio elevato.

Caso	Notificare l'autorità di controllo?	Notificare la persona interessata?	Note/raccomandazioni
Una multinazionale del commercio online viene fatta oggetto di un attacco informatico in seguito al quale vengono pubblicati in rete nomi utente, *password* e storia degli acquisti.	Sì. Segnalare il problema all'autorità centrale di controllo in presenza di dati transfrontalieri.	Sì, in quanto ciò potrebbe causare alti livelli di rischio.	Il titolare del trattamento deve intervenire, ad esempio forzando il ripristino delle *password* dei conti interessati, oppure seguire altri *step* per ridurre il rischio.
Un'azienda di *web hosting* (un responsabile del trattamento) identifica un errore nel codice che controlla l'autorizzazione utenti. Il risultato è che ogni utente può accedere ai dettagli dell'*account* di qualsiasi altro utente.	Come responsabile del trattamento l'azienda di web hosting deve immediatamente notificare i propri clienti (i titolari del trattamento) interessati. Dato per scontato che l'azienda di web hosting abbia condotto una propria indagine, i titolari del trattamento interessati devono essere ragionevolmente sicuri se abbiano o meno subito una violazione e, pertanto, se possano ritenersi "a conoscenza" una volta informati dall'azienda di *web hosting* (responsabile del trattamento). A questo punto il titolare del trattamento deve informare l'autorità di controllo.	Se è probabile che non vi sia un elevato rischio per le persone, queste non devono essere notificate.	L'azienda di *web hosting* (responsabile del trattamento) deve tenere in considerazione eventuali altri obblighi di notifica, ad es. in base alla Direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS). Se non vi è alcuna evidenza che questa vulnerabilità venga sfruttata dal titolare del trattamento, una violazione notificabile potrebbe non essersi verificata. Tuttavia è probabile che sia registrabile ovvero che configuri una non conformità ai sensi dell'art. 32.
A causa di un attacco informatico in un ospedale le cartelle cliniche non sono disponibili per un arco di 30 ore.	Sì. L'ospedale è tenuto a segnalare un potenziale elevato rischio per il benessere e la *privacy* dei pazienti.	Sì. Notificare i soggetti colpiti.	

Caso	Notificare l'autorità di controllo?	Notificare la persona interessata?	Note/raccomandazioni
I dati personali di 5.000 studenti vengono erroneamente inviati a una *mailing list* che include oltre 1.000 persone.	Sì, notificare l'autorità di controllo.	Sì, notificare gli individui a seconda della portata e della tipologia di dati personali coinvolti e della gravità delle possibili conseguenze.	
Un'e-mail di *direct marketing* viene inviata ai destinatari nei campi "To:" o "Cc:" permettendo così a ciascun destinatario di visualizzare l'indirizzo di posta elettronica degli altri destinatari.	Sì. Potrebbe essere obbligatorio notificare l'autorità di controllo se è interessato un alto numero di individui, nel caso in cui siano rivelati dati sensibili (ad es. una *mailing list* di uno psicoterapeuta) oppure nel caso in cui altri fattori presentino rischi elevati (ad es. il messaggio e-mail contiene le *password* iniziali)	Sì, notificare gli individui a seconda della portata e della tipologia di dati personali coinvolti e della gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non sono stati rivelati dati sensibili e se sia stato rivelato solo un numero ridotto di indirizzi di posta elettronica.