COMUNE DI VERRUA PO
Provincia di Pavia - Regione Lombardia
CAP 27040 Tel 0385-96121 0385-950037 FAX 0385-96447
CCP 14778278 P. IVA 00471420182 E-mail comune.verrua@libero.it
Uffici: Via Vittorio Veneto n. 1

Proceduradi gestione delle violazioni dei dati personali

(Data Breach Policy)

Approvato con deliberazione di Giunta n. 55 del 08.11.2021

INDICE

1. PREMESSA

L'Ente ai sensi del Regolamento Europeo 2016/679 (da qui in avanti GDPR), è tenuto a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).
È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'ente e per poter riscontrare nei tempi e nei modi previsti dalla normativa europea l'Autorità Garante e/o gli interessati.

2. SCOPO

Lo scopo di questa procedura è di definire un flusso per la gestione delle violazioni dei dati personali trattati dall' ente in qualità di Titolare del trattamento (di seguito "Titolare del trattamento"). Queste procedure sono ad integrazione delle procedure adottate dal Titolare del trattamento in materia di protezione dei dati personali ai sensi della legislazione vigente.
Attuale normativa di riferimento:

- Regolamento Generale sulla protezione dei dati personali (UE) 2016/679
- Decreto Legislativo n. 196/2003, come novellato dal D.Lgs. n. 101/2018
- Regolamento per l'attuazione del Regolamento UE 2016/679 relativo alla protezione e trattamento dei dati personali
- Linee guida WP art. 29.

3. DEFINIZIONI

Ai fini della presente procedura, valgono le seguenti definizioni:

a) 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o dagli Stati membri".
b) Responsabile 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 ai sensi dell'art. 28 GDPR".
c) Incaricato del Trattamento: "La persona fisica che nell'ambito della struttura aziendale del Titolare è autorizzata a effettuare attività di trattamento di dati personali".

d) DPO: “Il Responsabile del Trattamento come individuato dalla Sezione 4 (artt. 37-39) del Regolamento (UE) n. 2016/679”.
e) Dato personale: “Qualunque informazione relativa a persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare 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, generica, psichica, economica, culturale o sociale”.
f) Trattamento: “Qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio 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 altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione”.

4. VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Una violazione di dati personali (ovvero data breach) è ogni infrazione alla sicurezza degli stessi che comporti - 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 dal Titolare del trattamento (art. 4, n. 12 del Regolamento UE n. 2016/679).

Eventi di Data Breach possono riguardare sia casi cui è connesso un rischio marginale (es. perdita di una chiavetta USB di un dipendente), che casi più critici di furto o perdita di interi database, quali, a titolo esemplificativo, le banche dati gestite o documenti presenti nei suoi archivi.

Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà del dipendente (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo “owner”;

- virus o altri attacchi al sistema informatico o alla rete;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

5. SOGGETTI DESTINATARI DELLA PROCEDURA DI GESTIONE DATA BREACH

Queste procedure sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento, quali:

- i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (di seguito genericamente denominati Destinatari interni);
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Destinatario interno che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR o di autonomo Titolare (di seguito genericamente denominati Destinatari esterni);

Tutti i Destinatari (interni ed esterni) devono essere debitamente informati dell'esistenza della presente procedura, mediante metodi e mezzi che ne assicurino la comprensione.
Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

6. GESTIONE EVENTO DI DATA BREACH

Ai sensi dell'articolo 33 del Regolamento UE n. 2016/679, il Titolare del trattamento, in caso di una violazione dei dati personali trattati dall'Ente, è tenuto:

1. informare il Garante Privacy entro e non oltre le 72 ore successive all'avvenuta conoscenza della violazione (a meno che non sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli interessati);

2. nel caso in cui tale violazione sia suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, ad informare senza ritardo gli stessi interessati.

Al fine di rendere effettivo il processo di notifica dell'evento di data breach, la presente viene resa nota a tutti coloro che nell'ambito del rapporto di lavoro e/o di collaborazione trattano Dati personali del Titolare del

trattamento.

Nella gestione di evento di Data Breach è richiesta la massima attenzione e sensibilità da parte di tutte le funzioni coinvolte.

È fatto obbligo a ciascun dipendente e collaboratore di segnalare immediatamente ogni caso di incidente informatico e/o ad archivi cartacei di cui sia venuto a conoscenza e ogni evento che potrebbe potenzialmente condurre ad una violazione di dati personali, **mediante la compilazione dell'Allegato A – Modulo di comunicazione interna Data Breach da inviare all'indirizzo di posta elettronica certificata del DPO** pubblicato sul sito istituzionale www.comune.verruapo.pv.it

6.1 PROCESSO DI GESTIONE DELL'INCIDENTE

Al fine di consentire una gestione efficace e tempestiva delle violazioni dei Dati personali, il Titolare del trattamento adotta un processo strutturato per la gestione dei casi di incidenti che prevede:

- Rilevazione e segnalazione dell'incidente;
- Analisi dell'Incidente;
- Risposta ed eventuale notifica del Data Breach;
- Registrazione dell'Incidente.

6.2 SEGNALAZIONE DELL'INCIDENTE

La rilevazione e segnalazione dell'Incidente è un obbligo per tutti i dipendenti e/o collaboratori del Titolare del trattamento.

Nel caso in cui si verifichi uno degli eventi sopradescritti o in tutti gli altri casi in cui il soggetto che tratta dati personali sia consapevole di altri eventi potenzialmente rischiosi per i documenti e gli archivi, è tenuto a informare immediatamente l'Unità Privacy che provvede- senza indugio - a darne notizia all'Amministratore di Sistema per gli incidenti informatici e gestendo direttamente gli incidenti occorsi agli archivi cartacei.

6.3 ANALISI DELL'INCIDENTE

A seguito della segnalazione, il Titolare ed il DPO effettuano una valutazione al fine di verificare che nell'incidente rilevato siano stati effettivamente violati Dati personali trattati dall'Ente, **utilizzando l'Allegato B – Modulo di valutazione del Rischio connesso al Data Breach** che dovrà essere esaminato unitamente all'Allegato A, tenendo in debita considerazione i principi e le indicazioni di cui all'art. 33 del GDPR.

La suddetta analisi è finalizzata alla raccolta ed identificazione delle seguenti informazioni:

- categorie di Interessati cui i Dati personali violati si riferiscono (ad esempio, utenti, dipendenti, fornitori, etc.);
- categorie di Dati personali compromessi (ad esempio, Dati personali, Dati particolari, Dati giudiziari);
- tipologia di incidente: violazione della riservatezza, disponibilità o integrità (ad esempio, accesso non autorizzato, perdita, alterazione, furto, *disc/osure* , distruzione , etc.).

Nell'ambito di tale analisi, il Titolare identifica le azioni di prima risposta da intraprendere nell'immediato per contenere gli impatti dell'incidente.

Nell'ambito dell'analisi dell'incidente, vengono identificate anche le seguenti informazioni:

- identificabilità degli Interessati i cui dati rappresentano l'oggetto della violazione;
- misure di sicurezza tecniche e organizzative che potrebbero aver parzialmente o *in toto* mitigato gli impatti relativi all'incidente;
- ritardi nella rilevazione dell'incidente;
- numero di individui interessati.

Sulla base dei suddetti parametri ed utili i criteri delineati nell'Allegato C – Calcolo del livello di rischio, si procede alla valutazione della gravità dell'incidente relativamente ai diritti ed alle libertà degli Interessati, a seconda della natura dei Dati personali (ad esempio, Dati Sensibili e/o Giudiziari), delle misure di sicurezza adottate, della tipologia di interessati (ad esempio, minori o altri soggetti vulnerabili).

6.4 RISPOSTA E NOTIFICA DEL DATA BREACH

La precedente fase di analisi dell'incidente di data breach fornisce gli strumenti necessari ad identificare e valutare le conseguenze negative e gli impatti causati dall'incidente rilevato.

Nel caso in cui dovesse risultare improbabile che l'incidente presenti rischi per i diritti e le libertà degli interessati, la notifica all'Autorità Garante risulta essere non obbligatoria. Tale valutazione è condivisa con il DPO.

Qualora al contrario dovesse risultare possibile che l'incidente abbia determinato una violazione dei dati che presenti rischi per i diritti e le libertà

degli Interessati, il Titolare, con il supporto del DPO, procede a predisporre la notifica all'Autorità Garante utilizzando il modello messo a disposizione dalla stessa e rinvenibile al seguente link:

https://www.garanteprivacy.it/documents/10160/0/Modello+notifica+Data+Breach.pdf/6d1fa433-88dc-2711-22ab-dd5d476abe74?version=2.0

La notifica viene effettuata all'Autorità Garante entro 72 ore dal momento in cui il Data Breach è stato rilevato.

La suddetta notifica contiene almeno le seguenti informazioni:

- natura della violazione dei dati personali *(disclosure,* perdita, alterazione, accesso non autorizzato, etc.);
- tipologie di Dati personali violati;
- categorie e numero approssimativo di Interessati cui i dati compromessi si riferiscono;
- nome e dati di contatto del DPO, che sarà l'interfaccia per Titolare del trattamento nei confronti dell'Autorità di controllo;
- probabili conseguenze della violazione dei Dati personali;
- descrizione delle misure che il Titolare del trattamento ha adottato o è in procinto di adottare al fine di mitigare le conseguenze del Data Breach;
- ove la stessa non sia presentata entro 72 ore dalla rilevazione, i motivi dell'eventuale ritardo nella comunicazione.

Qualora non sia stato possibile fornire contestualmente tutte le informazioni obbligatorie, il Titolare - con il supporto dell'Amministratore di Sistema (relativamente agli incidenti informatici che dovessero verificarsi) e del DPO - raccoglie quanto prima le informazioni supplementari e provvede ad integrare, senza ritardo, la notifica già inoltrata all'Autorità di Controllo.

Oltre a notificare il Data Breach all'Autorità Garante, deve essere valutata l'esigenza di procedere con la denuncia all'Autorità Giudiziaria competente, nonché con la notifica del Data Breach anche ai soggetti interessati i cui dati siano stati violati.

Per stabilire se sia necessario provvedere alla notifica agli Interessati, saranno valutati i seguenti fattori:

- il trattamento può comportare discriminazioni, furto d'identità, perdite finanziare, disturbi psicologici, pregiudizio alla reputazione, perdita di riservatezza dei Dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo;

- gli Interessati rischiano di essere privati dei loro diritti, delle libertà o venga loro impedito l'esercizio del controllo sui Dati personali che li riguardano;
- sono trattati Dati personali che rivelano l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;
- in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti al fine di creare o utilizzare profili personali;
- sono trattati Dati personali di persone fisiche vulnerabili, in particolare minori;
- il trattamento riguarda una notevole quantità di Dati personali e un vasto numero di Interessati.

La notifica agli Interessati sarà effettuata nel caso in cui la violazione di Dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, a meno che non sia verificata almeno una delle seguenti condizioni:

- sono state applicate adeguate misure tecniche e organizzative per proteggere i dati prima della violazione, in particolare quelle in grado di renderle non intelligibili per soggetti terzi non autorizzati (ad esempio, misure di cifratura);
- a valle della rilevazione del Data Breach, sono state adottate misure per impedire il concretizzarsi dei rischi per i diritti e le libertà degli Interessati;
- la notifica del Data Breach a tutti gli Interessati singolarmente comporta uno sforzo sproporzionato rispetto al rischio. In tal caso si valuterà comunque l'opportunità di procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati siano comunque informati con analoga efficacia.

Il Titolare, di concerto con il DPO, valuta di volta in volta, sulla base della tipologia e del numero di Interessati, il canale di comunicazione che appare più opportuno per trasmettere la notifica agli stessi.

La notifica agli Interessati deve contenere:

- nome e dati di contatto del DPO;
- descrizione delle probabili conseguenze della violazione;
- descrizione delle misure adottate o che l'Ente intende adottare per porre rimedio alla violazione e ridurre gli effetti negativi.

6.5 DATA BREACH RELATIVO A DATI PERSONALI TRATTATI IN QUALITA' DI RESPONSABILE DEL TRATTAMENTO

Qualora, a seguito di una segnalazione o nel corso dell'analisi preliminare dell'Incidente di Data Breach, il Titolare rilevasse che la violazione qualificabile come Data Breach riguardasse dati personali di titolarità di un soggetto terzo trattati dall'Ente in qualità di Responsabile del trattamento, procede a informare senza ingiustificato ritardo il soggetto terzo titolare del trattamento.

Nel dettaglio, la comunicazione al soggetto titolare del trattamento dovrà contenere quanto menole seguenti informazioni (oltre a quelle eventualmente richieste dallo stesso soggetto terzo titolare del trattamento):

- Descrizione della natura della violazione dei dati personali comprensiva, ove possibile, di informazioni in merito alle categorie e al numero di Interessati nonché alle categorie e al volume approssimativo di dati personali oggetto di violazione;
- Nome e dati di contatto del DPO;
- Descrizione delle possibili conseguenze della violazione;
- Descrizione di eventuali misure già adottate o di cui si prevede l'adozione per porre rimedio alla violazione di dati personali e per attenuarne i possibili effetti negativi.

La comunicazione sarà inviata al soggetto titolare del trattamento entro 48 ore dall'avvenuta rilevazione della violazione o nel minore termine eventualmente indicato dal soggetto titolare del trattamento.

7. PRESCRIZIONI PER LA PREVENZIONE DI DATA BREACH

Si adottano specifiche strategie per prevenire o minimizzare il verificarsi di Data Breach.

In primo luogo, occorre che tutti i soggetti nominati quali autorizzati al Trattamento siano consapevoli dei Dati personali che trattano attraverso i propri strumenti (anche cartacei) e dispositivi o a cui hanno accesso tramite i sistemi del Titolare del trattamento.

A tal fine, la presente procedura viene loro comunicata ed essi dovranno custodire tali Dati personali ed i relativi documenti con cura e in modo responsabile sia all'interno che all'esterno della propria area di lavoro.

ALLEGATO A – MODULO DI COMUNICAZIONE DATA BREACH

Modulo di comunicazione interna Data Breach da inviare all'indirizzo di posta elettronica certificata del DPO reperibile sul sito www.comune.verruapo.pv.it

Comunicazione di Data Breach	Note
Data scoperta violazione:	
Data dell'incidente:	
Luogo della violazione (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supportiportatili):	
Nome della persona che ha riferito della violazione:	
Dati di contatto della persona che ha riferito della violazione (indirizzo e-mail, numero telefonico): *In caso di destinatario esterno indicare la ragione sociale:*	
Denominazione della/e banca/che dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati:	
Categorie e numero approssimativo di interessati coinvolti nella violazione:	
Breve descrizione di eventuali azioni poste in essere al momento della scoperta della violazione:	
Responsabile del dipartimento:	
data:	

ALLEGATO B – MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL DATA BREACH

Assessment di gravità	A cura del DPO insieme con l'amministratore di sistema, Responsabile dell'ufficio coinvolto della violazione e il team privacy incaricato
Dispositivi oggetto del Data Breach (computer, rete dispositivo mobile, file o parte di un file, strumento di back up, documento cartaceo, altro).	
Modalità di esposizione al rischio (tipo di violazione): lettura (presumibilmente i dati non sono stati copiati), copia (i dati sono ancora presenti sui sistemi ma del titolare), alterazione (i dati sono presenti sui sistemi ma sono stati alterati), cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione), furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione), altro.	
Breve descrizione dei sistemi di elaborazione o di memorizzazione dati coinvolti, con indicazione della loro ubicazione.	
Se laptop è stato perso/rubato: quando è stata l'ultima volta in cui il laptop è stato sincronizzato con il sistema IT centrale?	
Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati violata?	
La violazione può avere conseguenze negative in uno dei seguenti settori enteli: operation, research, financial, legal, liability or reputation?	
Qual è la natura dei dati coinvolti? Compilare le sezioni sottostanti:	

o I dati particolari (come identificati dal Regolamento (UE) 2016/679 relative ad una persona viva ed individuabile: a) origine razziale o etnica; b) opinion politiche, convinzioni religiose o filosofiche; c) appartenenza sindacale; d) dati genetici; e) dati biometrici; f) dati giudiziari; g) relative alla salute o all'orientamento sessuale di una persona.	
oInformazioni che possono essere utilizzate per commettere furti d'identità (i.e. dati di accesso e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito);	
o Informazioni personali relative a soggetti fragili (i.e. anziani, disabili, minori);	
o Profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone;	
Altro:	
La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro dato economico o sociale significativo?	
Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali che li riguardano?	
Quali misure tecniche e organizzative sono adottate ai dati oggetto di violazione, dal punto di viste delle infrastrutture informatiche?	

Il Titolare del trattamento ha adottato piano di protezione a tutela dei dati personali ?	
Il Titolare del trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?	
Classificazione della violazione e motivazioni:	
Notificazione del Data Breach all'Autorità Garante	Si/NO Se sì, notificato in data: Dettagli:
Comunicazione del Data Breach agli interessati	Si/NO Se sì, notificato in data: Dettagli:
Comunicazione del Data Breach ad altri soggetti	Si/NO Se sì, notificato in data: Dettagli:

ALLEGATO C - 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*	Viene valutato se il dato si dovrà valutare se 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

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...)

ALLEGATO D – REGISTRO DEI DATA BREACH

Numero Violazione	Data Violazione	Natura della Violazione	Categoria di Interessati	Categoria di dati personali coinvolti	Numero approssimativo di registrazioni dati personali	Conseguenze della Violazione	Contromisure adottate	Notifica Autorità Garante Privacy (S/N)	Comunicazione ai soggetti interessati (S/N)