Camera di Commercio
Pavia

ALLEGATO 9
AL MANUALE DI GESTIONE DOCUMENTALE
CCIAA PAVIA

Approvato con

Determinazione del Commissario Straordinario

n. 9 del 23 marzo 2022

PROCEDURA DATA BREACH

CAMERA DI COMMERCIO
DI PAVIA

Modello operativo per la protezione dei dati personali

Procedura “Gestione Data Breach”

Sommario

1 Premessa

Per "*data breach*" si intende una **violazione dei dati personali** dipendente da una **violazione di sicurezza** che comporta **accidentalmente o in modo illecito** la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati stessi (trasmessi, conservati o comunque trattati dall'Ente)[1].
Ai sensi degli artt. 33 e 34 del GDPR, in caso di *data breach*, il Titolare del trattamento è tenuto a notificare la violazione al Garante, senza ingiustificato ritardo e, se possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. L'obbligo non ricorre qualora il Titolare sia in grado di dimostrare che è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Il Referente (interno) del Trattamento e/o il Responsabile del Trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. Il Titolare inoltre deve comunicare all'interessato la violazione dei dati personali senza indebito ritardo in caso di rischio elevato per i diritti e le libertà delle persone fisiche.

L'Ente, al fine di adeguarsi alle previsioni sopra riportate con la presente procedura definisce:
- un processo operativo di Notifica/Comunicazione di un data breach, articolato nelle fasi di Segnalazione, Rilevazione, Valutazione, Notifica e Comunicazione;
- una metodologia di analisi del rischio per i diritti e le libertà dell'interessato associato al Data Breach oggetto di analisi e strumenti operativi volti a valutare, tra l'altro, la necessità di effettuare la Notifica al Garante/la Comunicazione agli interessati.

2 Fasi e attività

Di seguito si riportano le fasi in cui si scompone il processo "Gestione delle violazioni di dati personali", con riferimento al relativo obiettivo.

Fasi	Obiettivo
1) Segnalazione	Rendere nota l'occorrenza di eventi o incidenti che si presume possano costituire violazione di dati personali
2) Rilevazione	Acquisire gli elementi necessari per verificare e confermare (o escludere) il sussistere di una effettiva violazione di dati personali
3) Valutazione	Valutare il grado di rischio associato alla violazione rilevata

[1]Definizione di Agenda Digitale (www.agendadigitale.eu)

4) Notifica e Comunicazione	Assicurare l'invio tempestivo di notifiche verso il Garante della violazione accertata e, se previsto, anche della comunicazione verso gli interessati coinvolti nella violazione

2.1 Segnalazione

Il processo di gestione delle violazioni di dati personali prende avvio con l'acquisizione di una segnalazione di un evento o incidente che può sottendere una possibile violazione di dati personali in accordo alle tipologie definite nel **paragrafo 4.1**.Si precisa che l'incidente, all'atto della presente fase di segnalazione, è un evento avverso accertato, che ha o può avere un significativo impatto per l'Ente, i propri utenti, i collaboratori, i partner o i fornitori.
Le funzioni interessate a questa fase sono tutti i soggetti, interni o esterni alla Camera, coinvolti e/o preposti al trattamento dei dati che assistono a eventi o incidenti potenzialmente qualificabili come violazione dei dati personali. La segnalazione deve essere inoltrata al Referente Privacy della Camera, previo coinvolgimento del Referente interno e/o del Responsabile del Trattamento, che avalla la segnalazione fornendo descrizione scritta dell'evento intercorso e attestando i trattamenti coinvolti nell'evento.

2.2 Rilevazione

La fase di rilevazione viene attivata a fronte di segnalazioni generate come descritto nel paragrafo precedente, oppure a fronte di situazioni anomale, riconducibili ad eventi quali quelli illustrati nel paragrafo 4.1 o in generale indicativi di una possibile violazione dei dati.

In entrambi i casi, il Referente Privacy:

- raccoglie ulteriori elementi anche di natura dimensionale (es. n° di interessati convolti dall'evento), al fine di fornire una vista il più completa possibile dell'evento accaduto;
- effettua una analisi sull'accaduto al fine di accertare se l'evento occorso abbia comportato una effettiva violazione dei dati:
  a tal fine si avvale della piena collaborazione di altri soggetti che siano in grado di fornire elementi utili per verificare l'effettiva sussistenza di una violazione coinvolgendo in particolare il Responsabile della Sicurezza Informatica (Responsabile Transizione Digitale) e il Responsabile della Sicurezza Fisica deputati alla gestione delle informazioni e della sicurezza con riferimento al trattamento dei dati personali, nonché il o i Referenti interni e/o Responsabili del Trattamento.
  Le funzioni coinvolte devono garantire tempestivamente il supporto richiesto
- se emergono elementi che escludano la violazione, procede con il consueto processo di gestione dell'anomalia; nessun'altra azione è richiesta per la gestione della presunta violazione;
  altrimenti
- se attesta l'effettiva sussistenza della violazione ne mette a conoscenza il Titolare e il DPO. In concomitanza con tale comunicazione si determina la decorrenza del tempo limite (72 ore) per l'eventuale notifica al Garante.

2.3 Valutazione

La valutazione del livello di rischio, per i diritti e le libertà delle persone fisiche, associato alla violazione rilevata, viene effettuata in stretta connessione con la fase di rilevazione della stessa. Il Referente Privacy valuta, utilizzando le metodologie e gli strumenti descritti nel paragrafo 4, l'impatto effettivo e potenziale dell'evento ed il rischio ad esso associato avvalendosi della collaborazione del Responsabile della Sicurezza Informatica, del Responsabile della Sicurezza Fisica, del o dei Referenti interni e/o Responsabili del Trattamento e dell'eventuale consulenza del DPO.
Il Referente Privacy procede quindi con le seguenti attività:

- predispone un rapporto sugli esiti dell'attività di valutazione del rischio da fornire al DPO e al Titolare;
- valuta la possibilità di applicare misure compensative che possano ridurre, se non eliminare, il rischio per gli interessati;
- nel caso di livello di rischio Medio o Alto, procede come indicato nella successiva fase di Notifica e Comunicazione;
- laddove il livello di rischio associato alla violazione sia valutato come Basso, la violazione di dati personali viene archiviata. Se necessario l'evento verrà gestito come un normale incidente di sicurezza o anomalia.

In ogni caso è necessario verificare che siano state identificate le cause che hanno prodotto la violazione e le misure di sicurezza necessarie per evitare che l'evento si ripeta in futuro.

2.4 Notifica e Comunicazione

In caso di valutazione di rischio Medio o Alto, il Referente Privacy – verificata la disponibilità di tutte le informazioni necessarie – predispone la notifica verso il Garante e, se previsto, la comunicazione verso gli interessati coinvolti nella violazione di dati personali rilevata.

La notifica al Garante dovrà contenere, così come richiesto dall'art. 33 del GDPR, al minimo le seguenti informazioni:

- la descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Tutte le informazioni inerenti la violazione e la bozza di notifica al Garante vengono inviate al DPO.

Il Referente Privacy acquisisce e verbalizza il parere del DPO sulle informazioni inerenti la violazione e le eventuali modifiche alla notifica e procede al coinvolgimento del Titolare.
Il Titolare provvede quindi all'invio al Garante della notifica sulla violazione di dati personali accertata.
Tale notifica deve essere effettuata entro 72 ore dalla conoscenza della violazione che decorrono dall'attestazione della sua effettiva sussistenza come previsto nel precedente paragrafo 2.2. In

caso di invio della notifica al Garante oltre le 72 ore stabilite (es. raccolta delle informazioni sulla violazione alquanto onerosa), la notifica dovrà essere opportunamente corredata con le motivazioni che hanno indotto il ritardo.

In caso di violazioni catalogate di rischio Alto, il Referente Privacy valuta – in collaborazione con il DPO - la sussistenza di una delle condizioni di cui al comma 3) lettere a) e b) dell'art. 34 GDPR o viceversa la necessità di procedere con la comunicazione agli interessati della violazione rilevata nonché le modalità della stessa tenendo conto della numerosità e tipologia degli interessati.
In tal caso predispone la comunicazione agli interessati che descriva in maniera chiara ed esaustiva la violazione accaduta, le cause che l'hanno provocata e le misure che l'azienda ha deciso di mettere in campo per evitare che si ripeta nel futuro.
La comunicazione agli interessati avviene ad opera del Titolare con invio personale attraverso il mezzo considerato più idoneo (es. posta ordinaria, posta elettronica, SMS, Messaggi). I referenti di pertinenza provvedono ad estrarre i dati necessari per effettuare l'invio della comunicazione (es. indirizzi/recapiti postali, indirizzi di posta elettronica, numeri di telefoni/cellulari, ecc.).

Qualora la trasmissione personale richieda sforzi sproporzionati, la comunicazione agli interessati potrà avvenire in forma pubblica, o simile, sui media ritenuti più idonei (es. siti istituzionali dell'azienda, giornali, televisioni, radio).
In tal caso l'invio della comunicazione è affidato alle UO Responsabili del portale e delle relazioni con i media.

3 Matrice dei ruoli coinvolti

Ruolo / Fasi	Referente Privacy	Referenti interni e/o Responsabili del Trattamento	Responsabili della Sicurezza Informatica e Fisica	Soggetti interni ed esterni	Data Protection Officer	Responsabili della Comunicazione	Titolare
1) Segnalazione	x	x		X			
2) Rilevazione	x	x	x		x		
3) Valutazione	x	x	x		x		
4) Notifica e Comunicazione	x				x	x	x

4 Metodologia e strumenti

L'approccio metodologico per la gestione delle violazioni di dati personali si articola in tre parti distinte:

- la prima parte definisce le tipologie di violazioni di dati personali possibili e fornisce una tassonomia dei potenziali eventi che possono causare le violazioni;
- la seconda parte definisce gli scenari di rischio, con associati gli obblighi di notifica/comunicazione, nella quale una violazione si colloca;
- la terza parte identifica i criteri da utilizzare per la valutazione della violazione e il suo collocamento in alcuni scenari di rischio definiti.

4.1 Tipologia di violazione e tassonomia eventi

Una violazione dei dati personali è definita tale se ha un reale impatto sulla confidenzialità, integrità o disponibilità dei dati personali attinenti e coinvolti nella violazione. Le violazioni sono associate a un evento certo (o "ragionevolmente" certo). È opportuno precisare che il verificarsi di uno o più degli eventi di seguito descritti non costituisce una condizione sufficiente per determinare l'effettiva violazione dei dati personali, ma rappresenta un indicatore per l'identificazione dei casi da monitorare e analizzare.

4.1.1 Tipologia di violazione

Di seguito si riportano le tipologie di violazione dei dati personali che possono verificarsi.

Tipologia di violazione	Descrizione
1) Distruzione	Indisponibilità irreversibile o di lunga durata di dati personali trattati dal Titolare. La violazione può essere relativa a: • eliminazione logica non autorizzata (es. cancellazione dei dati) • eliminazione fisica (es. danneggiamento o distruzione dei supporti di memorizzazione o dei documenti cartacei) • eliminazione logica o fisica dei dati in formato elettronico, il cui ripristino da documenti cartacei è possibile ma con un impiego di tempo elevato, tale da poter generare effetti sull'interessato. In questo scenario, i dati personali possono essere recuperati solo: • direttamente dall'interessato; • da fonti esterne quali fonti pubbliche e/o di terze parti (es: Pubbliche Amministrazioni); • da archivi cartacei (in caso di distruzione, il recupero da tali archivi si suppone estremamente complesso, di lunga durata e con il rischio di ottenere dati non aggiornati). In alcuni casi la Distruzione può seguire a un Accesso ai dati da parte di soggetti non aventi diritto. In altri casi può essere dovuta ad errori nel trattamento.

Tipologia di violazione	Descrizione
2) Alterazione	Alterazione non autorizzata dei dati, che può determinare: • la comunicazione di informazioni erronee a enti esterni all'azienda (es. istituzioni, società, persone, ecc..) o al pubblico (Internet); • errori nel trattamento o trattamento non conforme; • decisioni errate con effetti sull'interessato. In alcuni casi l'Alterazione può seguire un Accesso ai dati da parte di soggetti non aventi diritto. In altri casi può essere dovuta ad errori nel trattamento.
3) Indisponibilità	Indisponibilità, irreversibile o temporanea, dei mezzi e degli strumenti necessari per effettuare il trattamento dei dati da parte degli interessati o del Titolare per l'erogazione di servizi richiesti o per conto dell'interessato. L'Indisponibilità non implica la Distruzione dei dati personali. L'Indisponibilità irreversibile di un mezzo o strumento richiede l'adozione di nuovi mezzi o strumenti per accedere ai dati. Tale violazione può essere relativa a: • indisponibilità dei sistemi e dei servizi informatici mediante i quali le informazioni sono accessibili (es: in caso di attacco informatico) • indisponibilità di mezzi e strumenti necessari per l'accesso alle informazioni (es: perdita di una chiave di decifratura o di un token hardware di accesso con la possibilità di accedere ai dati in backup o altri archivi) • indisponibilità degli strumenti atti a identificare l'informazione all'interno di grandi archivi cartacei o elettronici • degrado prestazionale dei servizi informatici, che determina l'impossibilità di perfezionare operazioni di trattamento • modifiche tecnologiche che rendono impossibile la decodifica di dati rappresentati secondo particolari formati di memorizzazione.

Tipologia di violazione	Descrizione
4) Perdita	Perdita del supporto fisico di memorizzazione dei dati (es. privazione, sottrazione, smarrimento dei dispositivi contenti i dati oppure dei documenti cartacei). La Perdita di un supporto fisico di memorizzazione dei dati non implica che si sia verificata anche un'altra violazione quale Distruzione, Indisponibilità, Accesso o Divulgazione: ad esempio, un disco DVD perso può contenere una copia cifrata[2] di dati.
5) Accesso	Effettivo accesso (anche in sola visualizzazione) ai dati trattati dalla Camera da parte di soggetti non aventi diritto al momento della violazione. L'accesso ai dati non implica che si sia verificata anche un'altra violazione quale Distruzione, Alterazione o Divulgazione: il soggetto non avente diritto potrebbe utilizzare a proprio favore le informazioni ricavabili dai dati senza distruggerli, alterarli o divulgarli.
6) Divulgazione	Comunicazione o diffusione non autorizzate o improprie dei dati personali, non corrispondenti a informazioni di pubblico dominio, verso terze parti, anche se non note o identificabili. In alcuni casi la Divulgazione può seguire un Accesso ai dati da parte di soggetti non aventi diritto. In altri casi può essere dovuta a trattamenti non conformi di dati riservati.

4.1.2 Tipologia di eventi

Di seguito si riportano le tipologie di eventi che possono generare una violazione dei dati personali, di cui si fornisce di seguito una tassonomia.

Tipologia di eventi	Descrizione
1) Eventi accidentali nei trattamenti elettronici dei dati	Eventi anomali determinati da fatti fortuiti nell'ambito dei trattamenti informatizzati, effettuati sui dati personali gestiti dall'azienda. Possono generarsi nell'ambito delle attività di gestione nei sistemi e delle infrastrutture IT sia svolte internamente che esternalizzate ad una terza parte. I motivi possono essere molteplici e tra questi si evidenziano le errate configurazioni dei sistemi e dei PC, la mancata o errata applicazione di policy o procedure di sicurezza, la distrazione e/o esecuzione erronea di operazioni, l'esaurimento del ciclo di vita delle componenti hardware, il danneggiamento delle componenti hardware, i malfunzionamenti software, la comunicazione o diffusione erronee di dati a soggetti non autorizzati, l'interruzione di servizi informatici, la modifica erronea di informazioni, basi di dati, archivi, autorizzazioni all'accesso, ecc.

[2] La cifratura dei dati, per essere efficace, richiede che le chiavi di cifratura siano integre, non violate e non divulgate.

Tipologia di eventi	Descrizione
2) Eventi accidentali nei trattamenti cartacei dei dati	Eventi anomali determinati da eventi fortuiti o comportamenti non dolosi nell'ambito dei trattamenti non automatizzati effettuati sui archivi cartacei di dati personali dell'azienda. Tra questi si evidenziano lo smarrimento o distruzione accidentale di documenti (es. incendio, allagamento locali, ecc), la comunicazione o diffusione erronee di dati a soggetti non autorizzati, la modifica erronea, il mancato aggiornamento dei dati, ecc.
3) Eventi dolosi	Comportamenti dolosi da parte di personale interno o soggetti esterni, anche per finalità di frode, sfruttando intenzionalmente un accesso legittimo ai dati, ai sistemi ed agli archivi cartacei, oppure mediante accesso non autorizzato ai dati attraverso il furto di credenziali o dispositivi, lo sfruttamento di vulnerabilità presenti sui sistemi, la compromissione di credenziali di autenticazione, l'utilizzo intenzionale (e pregiudizievole) di software oppure utilizzando comportamenti dolosi nell'ambito di trattamenti cartacei. Tali eventi possono includere i furti di supporti di archiviazione/elaborazione contenenti dati personali (es. furto di PC portatili, hard disk, chiavette USB, smartphone, tablet, ecc.) ed il furto di documenti cartacei.

4.2 Scenari di rischio

In conformità con i requisiti normativi, una violazione dei dati personali deve essere notificata al Garante per la Protezione dei Dati Personali ogni qualvolta essa "*presenti la possibilità del manifestarsi di un rischio per i diritti e le libertà delle persone fisiche*". Se tale rischio è valutato essere rilevante, il Titolare del trattamento deve comunicare la violazione anche all'interessato. Per tale ragione, si identificano 3 diversi scenari di rischio che corrispondono a diversi combinazioni di notifica/comunicazione. A tali scenari di rischio sono associati, oltre al livello di rischio, una descrizione, gli impatti sugli interessati dalla violazione e le notifiche/comunicazioni da inviare rispettivamente al Garante per la Protezione dei Dati Personali e all'interessato ad essi correlate.

Livello di rischio	Descrizione	Impatti su Interessato	Azioni previste
Basso	La tipologia della violazione e dei dati oggetto della violazione non implicano alcun rischio (o implicano un rischio trascurabile) per i diritti e le libertà degli interessati dovuto alla perdita della riservatezza, integrità e disponibilità dei dati personali.	Impatti improbabili o nulli sui diritti e sulle libertà degli interessati	Nessuna notifica/comunicazione
Medio	La tipologia della violazione e dei dati oggetto della violazione implicano un rischio medio per i diritti e le libertà degli interessati dovuto alla perdita della riservatezza, integrità e disponibilità dei dati	Impatti possibili ma limitati o scarsi, sui diritti e sulle libertà degli interessati	Notifica al Garante per la Protezione dei Dati Personali
Alto	La tipologia della violazione e dei dati oggetto della violazione implicano un rischio alto per i diritti e le libertà degli interessati coinvolti nella violazione dovuto alla perdita della riservatezza, integrità e disponibilità dei dati	Possibili impatti elevati sui diritti e sulle libertà degli interessati	Notifica al Garante per la Protezione dei Dati Personali Comunicazione agli interessati coinvolti nella violazione

Figura 1 - Scenari di rischio e azioni previste.

4.3 Criteri per la valutazione di una violazione

La valutazione dello scenario di rischio nel quale si colloca una violazione dei dati personali viene effettuata utilizzando una serie di criteri relativi a:

- tipologia/natura dei dati oggetto della violazione;
- tipologia della violazione;
- misure di sicurezza applicate ai dati sia prima della violazione che dopo.

Tali criteri sono stati correlati insieme in una matrice decisionale che consente in maniera agevole di identificare lo scenario di rischio nel quale si colloca la violazione e le notifiche/comunicazioni da effettuare.

I criteri utilizzati per l'identificazione dello scenario di rischio di una violazione sono:

- **Tipologia dei dati oggetto della violazione**: sono stati previsti tre diversi gradi di criticità associati alla tipologia dei dati trattati sulla base della loro rilevanza rispetto ai diritti e alle libertà delle persone fisiche:
  - **dati con criticità bassa**: sono generalmente dati personali comuni, più o meno

conoscibili o deducibili, ovvero che non contengono informazioni strettamente riservate la cui diffusione possa essere fortemente lesiva dei diritti e delle libertà dell'interessato stesso (es. dati anagrafici, dati di contatto, informazioni contrattuali, informazioni di marketing, e così via) o che l'interessato stesso non consideri particolarmente attinenti alla propria riservatezza (come per dati fiscali, contabili o relativi al censo). Sono dati con criticità bassa anche informazioni non essenziali per consentire l'erogazione di servizi o per prendere decisioni con effetti sull'interessato;

- **dati con criticità media**: dati che recano informazioni difficilmente conoscibili o deducibili della persona o che la persona ritiene particolarmente rilevanti per la propria privacy (es. la retribuzione, l'ammontare dei premi, procedimenti civili, accordi contrattuali, proprietà e disponibilità, aggregazione di informazioni – come l'acquisto o l'utilizzo di servizi - atte a ricostruire abitudini, comportamenti o specifici eventi avvenuti nel passato, la conoscenza di persone, la convivenza o la coabitazione, provvedimenti disciplinari, ecc.); sono dati con criticità media informazioni che possono influire nella corretta erogazione dei servizi o che possono causare decisioni errate con effetti limitati sull'interessato;
- **dati con criticità alta**: dati particolari (informazioni sulla salute, dati biometrici, dati genetici, procedimenti giudiziari, dati di traffico telefonico e telematico, dati di localizzazione e così via) o informazioni che possono essere utilizzate per perpetrare una frode, causare un danno o ledere la dignità o commettere un reato nei confronti della persona (es. numeri carte di credito, credenziali di accesso ai sistemi informatici, ecc.); sono dati determinanti per erogare correttamente un servizio o su cui si basano in modo significativo decisioni che possono avere effetti significativi sull'interessato.

Il livello di criticità dei dati deve anche tenere conto dei seguenti ulteriori tre fattori peggiorativi dello scenario di rischio:

- Numerosità dei dati coinvolti nella violazione per interessato;
- Particolari caratteristiche degli interessati quali: gruppi di persone particolarmente vulnerabili, come minori, anziani e categorie di persone affette da particolari sindromi o in particolari condizioni economiche;
- Particolari caratteristiche del titolare: questo fattore è rilevante in particolare quando una violazione in un'azienda del gruppo è gestita dalla capogruppo e deve essere valutato se l'ambito di attività del titolare, ad esempio ospedaliero, comporta un peggioramento dello scenario di rischio.

- **Criteri di classificazione della violazione**: I criteri forniti per la classificazione dei dati sono indicativi e possono variare in base al contesto nel quale sono collocati. Nel caso di dubbi, si suggerisce di posizionarsi cautelativamente sul livello più critico:
  - **Tipologia di violazione** così come descritta nel paragrafo 4.1;
  - **Identificabilità**, intesa come possibilità di identificare puntualmente un soggetto sulla base dei dati oggetto della violazione (es: presenza di codici identificativi della persona piuttosto che di una pratica, o esplicito riferimento ai dati di contatto);
  - **Misure di sicurezza messe in atto** per proteggere i dati (es. cifratura / anonimizzazione dei dati, separazione dei dati, autenticazione forte, ecc.);
  - **Misure di mitigazione del danno** poste in essere a seguito del verificarsi della violazione a riduzione del rischio del ripetersi dell'evento di violazione e per scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati (es. modifica/creazione credenziali di accesso ai dati, cancellazione sicura dei dati oggetto di violazione, cifratura dei dati oggetto di violazione, ecc.);
  - **Numero di interessati coinvolti**: numero di persone a cui si riferiscono i dati oggetto di

violazione. Tale parametro non determina necessariamente l'obbligo di comunicazione, ma costituisce un elemento discriminante per considerare la violazione dei dati personali sufficientemente grave per procedere con una Notifica. In determinati casi, il furto di dati afferenti ad un numero elevato di persone può caratterizzare anche la natura delle possibili conseguenze per gli interessati (ad esempio, la raccolta di numerosi dati per la conduzione di campagne di phishing o per adottare pratiche di concorrenza sleale anche attraverso comportamenti scorretti verso gli interessati, come l'esecuzione di campagne di marketing aggressive). Tale parametro ha anche effetto sulle modalità che dovranno essere previste in caso di Comunicazione agli interessati, come previsto dalla normativa.

I criteri sopra descritti sono stati correlati nella **matrice decisionale** allegata al presente documento che consente, in maniera agevole, di identificare lo scenario di rischio nel quale la violazione in esame si colloca. Per agevolare l'utilizzo della tabella, sono riportate di seguito delle note esplicative per l'utilizzo.

4.4 Note esplicative per l'utilizzo della Matrice Decisionale allegata

Per utilizzare la tabella di correlazione allegata, è necessario eseguire in sequenza le attività qui di sotto elencate leggendo la tabella da sinistra a destra:

1) Partire dalla prima colonna di sinistra "**Tipologia della Violazione",** scegliere il tipo di violazione tra i casi descritti al paragrafo 4.1: Distruzione, Indisponibilità, Perdita, Alterazione, Divulgazione e Accesso; nel caso la violazione comporti più tipi di violazioni, ripetere la procedura per ogni tipo di violazione coinvolto ed utilizzare il risultato con criticità più alta tra quelli ottenuti;
2) Procedere verso destra alla seconda colonna "**Identificabilità degli interessati"**, analizzare i dati coinvolti nella violazione al fine di comprendere il grado di identificabilità dell'interessato a partire da questi (vedi paragrafo 4.3); quando è indicato "Non rilevante", significa che per quella tipologia di violazione, tale parametro non concorre all'identificazione dello scenario di rischio;
3) Procedere verso destra alla terza colonna "**Misure di Sicurezza Applicate (pre-violazione)**", analizzare le misure di sicurezza applicate pre-violazione ed identificare quelle implementate; quando è indicato "Non rilevante", significa che per quella tipologia di violazione tale parametro non concorre all'identificazione dello scenario di rischio;
4) Procedere verso destra alla quarta colonna "**Controlli di mitigazione (post-violazione)**", analizzare i controlli di mitigazione applicati post violazione ed identificare quelli implementati; quando è indicato "Non rilevante", significa che per quella tipologia di violazione, tale parametro non concorre all'identificazione dello scenario di rischio;
5) Procedere verso destra alla quinta colonna "**Dati di pubblico dominio**", per alcuni tipi di violazione e scenario, il livello di rischio dipende se i dati sono solo di dominio pubblico oppure vi sono dati anche o esclusivamente non pubblici: identificare il caso rilevante per lo scenario in analisi; quando è indicato "Non rilevante", significa che per quella tipologia di violazione tale parametro non concorre all'identificazione dello scenario di rischio;
6) Procedere verso destra alla sesta colonna "**Numero di interessati coinvolti"** - Identificare il numero di interessati coinvolti, generalmente in termini di ordini di grandezza nella scala Basso, Medio, Alto; indicativamente:

a. **Basso**: il numero di interessati coinvolti è inferiore al 20% di tutti i possibili interessati;
b. **Medio**: il numero di interessati coinvolti è maggiore o uguale al 20% e inferiore al 80% di tutti i possibili interessati;
c. **Alto**: il numero di interessati coinvolti è maggiore o uguale al 80% di tutti i possibili interessati;

quando è indicato "Non rilevante", significa che per quella tipologia di violazione, tale parametro non concorre all'identificazione dello scenario di rischio;

7) Procedere verso destra alle ultime tre colonne "**Tipologia Dato**" ed identificare, secondo quanto descritto nella sezione 4.3, la criticità dei dati coinvolti nella violazione; identificata la colonna di Criticità Bassa, Media o Alta, intersecare questa colonna con la riga identificata ai punti precedenti, determinando così lo scenario di rischio, vedi paragrafo 4.2, che consente di determinare le tipologie di notifica/comunicazione da effettuare verso il Garante per la Protezione dei Dati Personali e verso gli interessati dei dati coinvolti nella violazione.

5 Appendice

5.1 Riferimenti normativi

Regolamento UE 679/2016

Articolo 33 - Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il referente interno e/o il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
   a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
   b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati (DPO) o di altro punto di contatto presso cui ottenere più informazioni;
   c) descrivere le probabili conseguenze della violazione dei dati personali;
   d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34 - Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
   a. il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
   b. il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
   c. detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Article 29 Data Protection Working Party WP250

Nelle Linee Guida WP250 adottate il 3 ottobre 2017, il Article 29 Data Protection Working Party complementa il Regolamento UE 679/2016 con alcune indicazioni pratiche per la gestione dei Data Breach. Nelle Linee Guida si ricorda che i principi di sicurezza la cui violazione comporta un Data Breach sono: Confidenzialità, Integrità e Disponibilità dei dati. Le Linee Guida indicano inoltre che la severità di una violazione ed i conseguenti rischi per i diritti e le libertà delle persone fisiche possono essere valutati sulla base di:

- tipologia della violazione
- natura, sensibilità e numerosità dei dati
- facilità di individuazione degli interessati
- severità delle conseguenze per gli interessati
- particolari caratteristiche degli interessati
- numero degli interessati coinvolti
- particolari caratteristiche del titolare.

6 Allegati

Descrizione	Nome file
Flusso	Procedura Gestione Data Breach - Flusso
Matrice Decisionale	Procedura Gestione Data Breach - Matrice Decisionale