Camera di Commercio
Pavia

PROCEDURA DI GESTIONE
DATA BREACH

Approvata con Determinazione del Commissario Straordinario n. ….. del …….

Il presente documento si colloca nelle azioni *accountability* dell'Ente, in linea con i principi di cui al **Regolamento (UE) 2016/679 – GDPR**

SOMMARIO

INTRODUZIONE AL DOCUMENTO

SCOPO E CAMPO DI APPLICAZIONE

Scopo della presente Procedura è descrivere compiti e responsabilità nel processo di gestione delle violazioni dei dati personali (c.d. *Data Breach*) nel rispetto delle disposizioni contenute nel Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito GDPR).

Tale processo si sviluppa nelle seguenti fasi:

a) rilevazione e inquadramento dell'incidente di sicurezza;
b) messa in atto delle strategie di contenimento dei rischi e delle eventuali azioni correttive;
c) svolgimento di ulteriore attività investigativa volta a individuare le conseguenze e/o i possibili rischi per i diritti e le libertà delle persone fisiche;
d) eventuale notificazione del *Data Breach* all'Autorità Garante ai sensi dell'art. 33 GDPR e in conformità con le previsioni della WP 250 del 6 febbraio 2018;
e) eventuale comunicazione agli Interessati coinvolti, quando la violazione dei dati personali presenta un rischio elevato per i loro diritti e libertà;
f) registrazione dell'evento ai sensi dell'art. 33, par. 5, GDPR, al fine di documentare qualsiasi violazione dei dati personali comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

La presente Procedura si applica, per quanto compatibile, anche laddove:

1. la violazione coinvolga **dati trattati in regime di contitolarità**, salvo diverse indicazioni o procedure operative indicate dall'accordo di contitolarità o comunque fissate nell'ambito del relativo rapporto instauratosi;
2. l'Ente operi in **qualità di Responsabile del trattamento**, ex art. 28 del GDPR; in tal caso, oltre a dover essere osservate anche le indicazioni ed istruzioni fornite dal Titolare nel relativo atto di nomina, le fasi relative alla notifica al Garante e alla comunicazione agli interessati sono attuate direttamente dal Titolare del Trattamento seguendo proprie procedure; Responsabile mantiene in ogni caso precisi obblighi di comunicazione e collaborazione nei confronti del Titolare.

La presente Procedura è portata a conoscenza, anche attraverso attività di sensibilizzazione o formazione, a tutti i Dirigenti, funzionari o, comunque, referenti delle Aree/Servizi/Uffici della Camera di Commercio, Industria, Artigianato e Agricoltura di Pavia (di seguito, più semplicemente "CCIAA di Pavia".

RIFERIMENTI NORMATIVI

La presente Procedura risponde ai seguenti requisiti normativi:

1. Regolamento UE 2016/679 "Regolamento generale sulla protezione dei dati personali";
   - art. 33 GDPR - Notifica di una violazione dei dati personali all'autorità di controllo;
   - art. 34 GDPR - Comunicazione di una violazione dei dati personali all'interessato;
2. Decreto legislativo n. 196/2003 "Codice in materia di protezione dei dati personali", come modificato dal D.Lgs. n.101/2018;
3. Linee Guida in materia di notifica delle violazioni dei dati personali - WP250 rev.01, *Guidelines on Personal Data Breach notification under Regulation 2016/679*, aggiornata al 06/02/2018;
4. Provvedimenti emessi dall'Autorità Garante; in particolare, il Provvedimento n° 209 del 27 maggio 2021, relativo alla nuova Procedura telematica per la notifica di violazioni di dati personali (doc. web n. 9667201).

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR / Regolamento	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice *privacy*	D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018
Garante	Autorità Garante per la protezione dei dati personali
WP29 / EDPB	Già *Article 29 Data Protection Working Party* o Gruppo di lavoro *ex* art. 29, ora EDPB, *European Data Protection Board*
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
Interessato	La persona fisica cui si riferiscono i dati personali
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 degli Stati membri (art. 4, punto 7 del GDPR)
DPO	Data Protection Officer / Responsabile della protezione dei dati, ai sensi dell'art. 37 del GDPR
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
Designato	Soggetto a cui, ai sensi dell'art. 2-*quaterdecies* del Codice *privacy*, l'Ente ha attribuito specifici poteri, oltre che compiti e funzioni, ai fini non solo dell'esecuzione di attività materiali di trattamento, ma anche e soprattutto per contribuire ad assicurare la *compliance* dell'Ente al GDPR
Referente Privacy	Persona individuata dalla CCIAA per il coordinamento delle attività in ambito di privacy in carico
Amministratore di Sistema Interno	Persona fisica incaricata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, ivi comprese le figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi
SG	Segretario Generale della CCIAA
Incidente di sicurezza	Qualsiasi accadimento significativo per la gestione delle infrastrutture IT e per la gestione dell'operatività dei servizi
Violazione dei dati (*Data Breach*)	L'incidente di sicurezza 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 (art. 4, punto 12 GDPR)

MATRICE DELLE REVISIONI

Data	Descrizione
__.__.__	Nuova procedura *Data Breach*.

ACCORTEZZE A LIVELLO CONTRATTUALE

RESPONSABILI DEL TRATTAMENTO

Con riferimento ai soggetti che trattano dati per conto della CCIAA DI PAVIA – e sono dunque stati nominati dalla CCIAA DI PAVIA quali propri Responsabili (o sub-Responsabili) del trattamento – occorre che i relativi contratti / nomine poste in essere prevedano espressamente che:

- il Responsabile deve assistere la CCIAA DI PAVIA nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- se il Responsabile viene a conoscenza di una violazione dei dati personali che sta trattando per conto della CCIAA DI PAVIA, il Responsabile del trattamento deve darne comunicazione alla CCIAA DI PAVIA senza ingiustificato ritardo.

È opportuno precisare che il Responsabile del trattamento non deve valutare la probabilità di rischio derivante dalla violazione prima di comunicarla alla CCIAA DI PAVIA; spetta infatti a quest'ultima effettuare la valutazione nel momento in cui viene a conoscenza della violazione. Il Responsabile del trattamento deve limitarsi a stabilire se si è verificata una violazione e darne comunicazione alla CCIAA DI PAVIA.

Il regolamento non fissa un termine esplicito entro il quale il Responsabile del trattamento deve avvertire il Titolare del trattamento, salvo specificare che deve farlo "*senza ingiustificato ritardo*". Si suggerisce comunque di precisare nei contratti un termine massimo (in numero di ore) entro cui il Responsabile deve comunque dare comunicazione dell'avvenuta violazione a Titolare del trattamento, precisando che tale termine ha valore anche in periodi festivi.

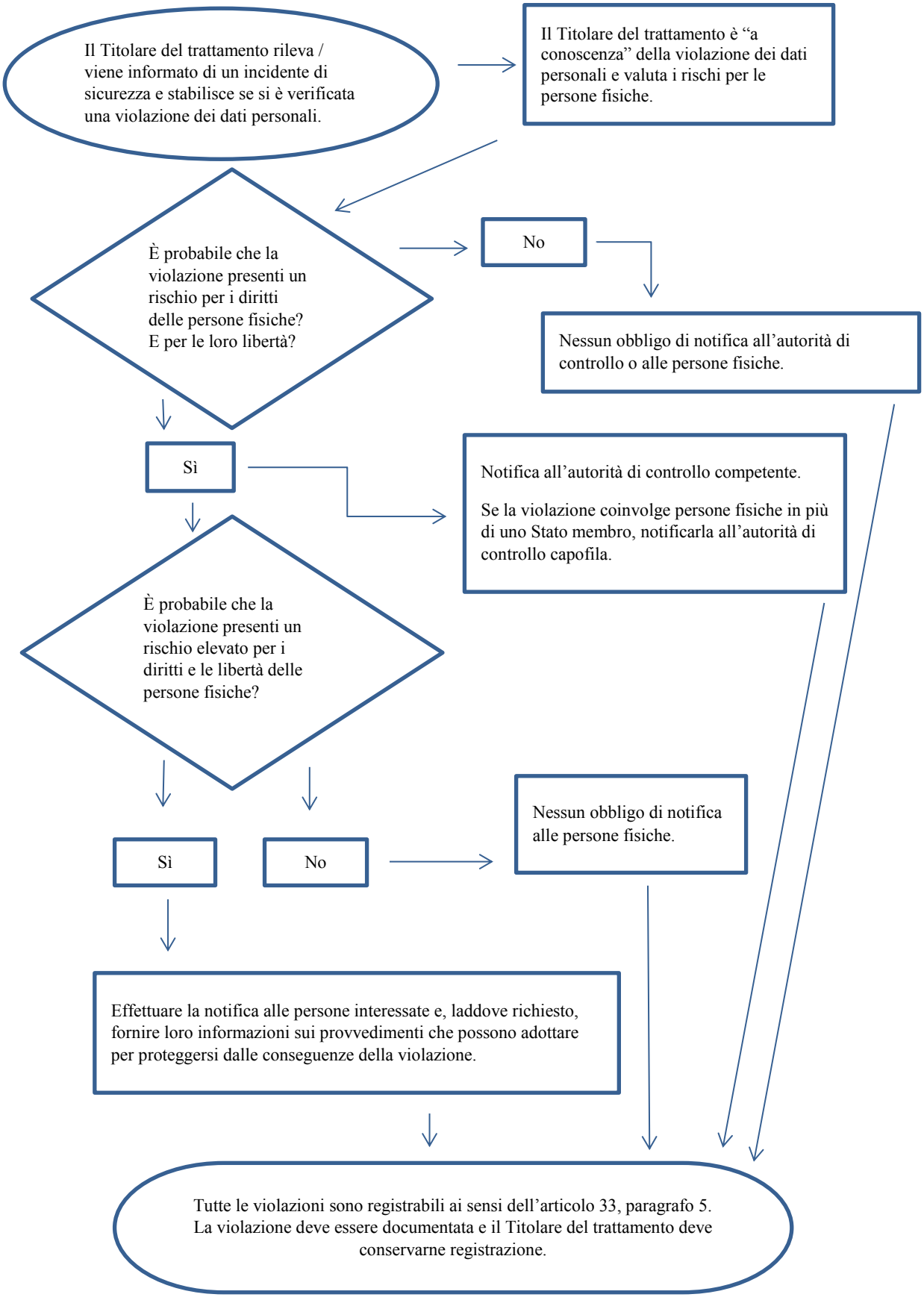
CONTITOLARI DEL TRATTAMENTO

In caso di contitolarità, è opportuno ricordare che l'art. 26 GDPR specifica che, nel relativo patto, occorre determinare le rispettive responsabilità in merito all'osservanza del Regolamento: ciò include la determinazione di chi sarà responsabile di adempiere agli obblighi di cui agli articoli 33 e 34 GDPR.

A tale proposito, il WP29 ha raccomandato che gli accordi contrattuali tra i contitolari del trattamento includano disposizioni che stabiliscano quale Contitolare del trattamento deve assumere il comando o è responsabile del rispetto degli obblighi di notifica delle violazioni previsti dal Regolamento.

FASI DEL PROCESSO DI GESTIONE DEI DATA BREACH

La gestione di un *Data Breach* può riassumersi nelle fasi di seguito rappresentate.



TIPOLOGIE DI RILEVAZIONE DEL DATA BREACH

La rilevazione di un incidente può essere di tre tipologie, a seconda del soggetto o del sistema che effettua la rilevazione:

↘ **RILEVAZIONE AUTOMATICA**: da sistemi di segnalazione automatica (es. SIEM - *Security Information and Event Management*), come le violazioni derivanti da superamento dei sistemi di Firewall della CCIAA DI PAVIA (gestiti direttamente o tramite soggetti esterni: p.es. InfoCamere o altri Responsabili del trattamento).

↘ **RILEVAZIONE INTERNA**: dai singoli dipendenti della CCIAA DI PAVIA o da attività di monitoraggio degli eventi da parte degli Amministratori di sistema interni; comunicazione di (anche solo sospetti) malfunzionamenti irrituali o blocco dei sistemi, furti, smarrimenti, intrusioni fisiche nei locali archivio, ecc.

↘ **RILEVAZIONE ESTERNA**: da parte di Responsabili del trattamento nominati ai sensi dell'art. 28 GDPR, di fornitori esterni e/o altri consulenti nell'ambito dell'attività di monitoraggio, assistenza e manutenzione prestata a favore della CCIAA DI PAVIA, oppure di utenti dei servizi della CCIAA DI PAVIA o, ancora, di soggetti terzi.

A CHI INOLTRARE LA SEGNALZIONE

Tutte le rilevazioni di *Data Breach* o sospetti tali devono comportare una segnalazione immediata da parte dei dipendenti della CCIAA DI PAVIA, corredata dal maggior numero di dettagli possibile, al Referente Privacy dell'Ente.

Chi effettua la segnalazione deve restare a disposizione e contattabile per eventuali necessità di chiarimento o per la richiesta di informazioni ulteriori, non trasmesse contestualmente alla segnalazione.

Ricevuta la segnalazione, il Referente Privacy, salvo sia evidente – al di là di ogni ragionevole dubbio – che la segnalazione non riguardi un possibile *Data Breach*, provvede preliminarmente ed immediatamente, sulla base delle informazioni a disposizione, a verificare quali aree dell'Ente sono state interessate o potrebbero essere interessate dal potenziale *Data Breach*, dandone immediato avviso ai Designati riferimento.

Successivamente, il Referente Privacy attiva il "Team *Data Breach*", come da indicazioni di seguito riportate.

FASE 1: COSTITUZIONE DEL "TEAM DATA BREACH" E PRIMI RILIEVI

Il Referente Privacy attiva il **Team *Data Breach*** (di seguito **TDB**) composto da:

- il **Segretario Generale (SG)-Responsabile Privacy** della CCIAA DI PAVIA, che presiede e dirige i lavori del Team;
- il **Referente Privacy** della CCIAA DI PAVIA;
- il **DPO** della CCIAA DI PAVIA;
- i Designati responsabili delle aree/funzioni coinvolte o potenzialmente coinvolte dalla violazione;
- il Referente informatico interno, ove l'evento riguardi l'infrastruttura IT, i sistemi informatici e/o le banche dati gestiti/e internamente dalla CCIAA DI PAVIA.

Detti soggetti, coordinandosi tra loro, anche senza necessità che si riuniscano fisicamente, devono – nel più breve tempo possibile – assumere ogni informazione utile a inquadrare la tipologia dell'incidente e, conseguentemente, accertare se tale evento ha coinvolto o meno dati personali.

Il **TDB**, ove necessario, si interfaccia direttamente con i Referenti delle Società e/o degli Enti coinvolte/i nell'incidente di sicurezza segnalato, operanti in qualità di Responsabili o di Contitolari del trattamento.

> Spetta al **Segretario Generale**, acquisito il parere (non vincolante) degli altri membri, decidere in relazione all'esito di tutte le valutazioni che seguono.
>
> Il Team deve dunque intendersi quale gruppo di supporto al SG, affinché questi possa assumere decisioni quanto più informate e consapevoli possibile.
>
> **Nell'ambito delle sole Fasi da 1 a 4** della presente Procedura (non per la Fase 5), il Segretario Generale può decidere, mediante comunicazione mail inoltrata (almeno) al Referente Privacy e al DPO, di farsi sostituire dal **Referente Privacy** interno. In tal caso, il Referente Privacy, nei limiti di cui alla comunicazione del SG, assume la direzione del **TDB** e (ove espressamente previsto dal SG) assume altresì le relative decisioni, dandone immediata comunicazione al SG.

In prima fase, il **TDB** deve provvedere ad assumere informazioni preliminari in relazione a:

1. il sistema, l'infrastruttura, l'applicazione, la banca dati oggetto dell'incidente di sicurezza;

2. la/le macro-tipologia/e di violazione verificatasi:
   - ☐ violazione della riservatezza dei dati
   - ☐ violazione dell'integrità dei dati
   - ☐ violazione della disponibilità dei dati

3. la tipologia di dati coinvolti (occorre stabilire se l'incidente ha coinvolto dati personali e, se sì, di quale/i categoria/e):
   - ☐ **assenza di dati personali**[1]
   - ☐ dati personali "comuni"

[1] In questo caso, l'evento non è qualificabile come *Data Breach*.

- ☐ dati personali "particolari" (art. 9 GDPR)
- ☐ dati personali "relativi a condanne penali e reati"

4. il volume dei dati e, ove possibile, il numero degli interessati coinvolti;
5. le misure di sicurezza (tecniche ed organizzative) in essere;
6. le attività di *remediation* (azioni correttive) attuabili immediatamente;
7. le attività di *remediation* (azioni correttive) ipotizzabili e/o future, anche al fine di non far più ripetere il medesimo evento o eventi similari.

ATTENZIONE: **dal momento in cui si è ragionevolmente certi che si sia verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali, la CCIAA DI PAVIA (ove Titolare del trattamento) si ritiene "a conoscenza" dell'avvenuto *Data Breach*. È da questo momento che decorre il termine di 72 ore per procedere – ove necessario – alla notifica all'Autorità garante per la protezione dei dati personali.**

In alcuni casi è fin dall'inizio relativamente evidente che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se sono stati effettivamente compromessi dati di carattere personale.

Come precisato nelle Linee guida WP250rev.01, in materia di *Data Breach*, ove una fonte esterna "*informa il Titolare del trattamento di una potenziale violazione o se egli stesso rileva un incidente di sicurezza, il Titolare del trattamento può effettuare una breve indagine per stabilire se la violazione si sia effettivamente verificata. Durante il periodo di indagine il titolare del trattamento non può essere considerato "a conoscenza". Tuttavia, si prevede che l'indagine iniziale inizi il più presto possibile e stabilisca con ragionevole certezza se si è verificata una violazione; può quindi seguire un'indagine più dettagliat*a".

Il **TDB** pone in essere tutte le necessarie strategie di contenimento dei rischi e le eventuali azioni di *remediation* (azioni correttive) immediate.

Nel caso in cui l'evento coinvolga dati personali, viene attivata la successiva fase che comporta lo svolgimento di attività investigativa volta ad individuare i possibili rischi per i diritti e le libertà delle persone fisiche.

Successivamente all'acquisizione di tutte le informazioni di cui sopra, ove l'incidente sia stato qualificato come *Data Breach* (e dunque sia effettivamente intercorso ed abbia coinvolto – o stia coinvolgendo – dati di carattere personale), il **TDB**, tenuto conto del **termine massimo di 72 ore** da quando la CCIAA DI PAVIA è venuta a conoscenza della violazione, procede secondo quanto descritto nelle fasi che seguono.

Ove l'evento interessi attività svolte dalla CCIAA DI PAVIA in qualità di Responsabile del trattamento o di Contitolare, è importante che il **TDB** effettui le valutazioni di cui sopra nel più breve tempo possibile e comunque entro il termine (eventualmente indicato nell'atto di nomina, nel patto o nel contratto) per la comunicazione del *Data Breach*, a seconda dei casi, al Titolare o al/i Contitolare/i.

FASE 2: INDAGINE CONOSCITIVA

Anche ai fini dell'eventuale compilazione della notificazione di avvenuto *Data Breach* all'Autorità garante per la protezione dei dati personali, è necessario che il **TDB** svolga d'urgenza un'indagine volta alla raccolta di ulteriori, approfondite informazioni relative all'accaduto.

Ove tale indagine richieda diverso tempo, tale da far superare il termine di 72 ore da quando la CCIAA DI PAVIA è venuta a conoscenza della violazione, il **TDB**, sentito in particolar modo il parare (non vincolante) del DPO, può optare per l'effettuazione di una notificazione parziale all'Autorità garante per la protezione dei dati personali, con riserva di integrare la stessa non appena completato il processo di raccolta delle informazioni (che dovrà comunque avvenire nel più breve tempo possibile). Si badi, a tale proposito, che sono anche possibili casi ove, successivamente alla notifica iniziale, il prosieguo delle indagini conoscitive dimostra che l'incidente di sicurezza è stato contenuto o, addirittura, che non si è verificata alcuna violazione di dati personali; anche in questi casi sarà necessario procedere all'integrazione della segnalazione, di modo che l'incidente possa essere registrato come un evento che non costituisce *Data Breach*: "*Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione*" (Linee guida WP250rev.01).

Di seguito, sono elencate le informazioni che il **TDB** deve obbligatoriamente raccogliere nel corso della propria indagine.

A.2) Elenco dei soggetti esterni coinvolti nel trattamento (Responsabili *ex* art. 28 e Contitolari del trattamento), comprensivo di denominazione e codice fiscale (per enti e imprese) o partita IVA (per professionisti).

A.3) Momento in cui è avvenuta la violazione.

A.4) Modalità e momento (data e ora) attraverso cui la CCIAA DI PAVIA è venuta a conoscenza della violazione.

A.5) Natura della violazione (perdita di riservatezza, integrità e/o disponibilità di dati).

A.6) Causa della violazione.

A.7) Descrizione della violazione.

A.8) Descrizione dei sistemi, software, servizi e delle infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione.

A.9) Descrizione delle misure tecniche e organizzative in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti.

A.10) Categorie di interessati coinvolti nella violazione (es. dipendenti, utenti, consulenti, minori, ecc.).

A.11) Numero (anche approssimativo) di interessati coinvolti nella violazione.

A.12) Categorie di dati personali su cui ha inciso la violazione:

- ☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
- ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
- ☐ Dati di accesso e di identificazione (username, password, customer ID, altro...)

- ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...)
- ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro...)
- ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
- ☐ Dati di profilazione
- ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro...)
- ☐ Dati di localizzazione
- ☐ Dati che rivelino l'origine razziale o etnici
- ☐ Dati relativi a opinioni politiche
- ☐ Dati relativi a convinzioni religiose o filosofiche
- ☐ Dati che rivelino l'appartenenza sindacale
- ☐ Dati relativi alla vita sessuale o all'orientamento sessuale
- ☐ Dati relativi alla salute
- ☐ Dati genetici
- ☐ Dati biometrici
- ☐ Altro

A.13) Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati.

A.14) Numero (anche approssimativo) di registrazioni dei dati personali oggetto di violazione (es. numero di fatture, ordini, referti, immagini, record di un database o numero di transazioni).

A.15) Verificare se la violazione riguarda un trattamento transfrontaliero di dati.

FASE 3: VALUTAZIONE DEI RISCHI

AVVERTENZA

Le tabelle di cui ai paragrafi che seguono non costituiscono un vincolo per il **TDB**, il quale resta libero di adottare i parametri di calcolo che ritiene più idonei per la valutazione di ciascun caso concreto.

Tuttavia, ove il **TDB** decida di discostarsi dalle tabelle previste dalla presente Procedura, per ragioni di *accountability* è necessario vengano verbalizzate le ragioni specifiche relative all'impiego di parametri diversi.

In generale (a prescindere da quali parametri il **TDB** decida di adottare) le valutazioni debbono, in particolare, tenere conto dei seguenti criteri:

Aspetti generali

Nel valutare il rischio che potrebbe derivare da una violazione, occorre considerare tanto la gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche, quanto la probabilità che tale impatto si verifichi.

Chiaramente, se le conseguenze di una violazione sono più gravi, il rischio è più elevato; analogamente, se la probabilità che tali conseguenze si verifichino è maggiore, maggiore è anche il rischio.

A seconda della natura dei dati personali coinvolti in una violazione, ad esempio categorie particolari di dati, il danno potenziale alle persone che potrebbe derivarne può essere particolarmente grave soprattutto se la violazione può comportare furto o usurpazione di identità, danni fisici, disagio psicologico, umiliazione o danni alla reputazione. Se la violazione riguarda dati personali relativi a persone fisiche vulnerabili, queste ultime potrebbero essere esposte a un rischio maggiore di danni.

Il fatto che il titolare del trattamento sappia o meno che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale: ad esempio, in caso di comunicazione di dati personali a destinatari erronei, se tali destinatari sono organizzazioni fidate e con cui si hanno rapporti stabili, domandando loro di restituire o distruggere in maniera sicura i dati ricevuti è possibile aspettarsi, ragionevolmente, che gli stessi non leggeranno o accederanno ai dati loro inviati. Ergo, la probabilità che detta violazione presenti un rischio per le persone fisiche verrebbe meno.

Infine, nella valutazione di gravità occorre tener conto anche della permanenza delle conseguenze negative per le persone fisiche: l'impatto potrebbe infatti essere considerato maggiore qualora gli effetti della violazione fossero "a lungo termine".

Tipo di violazione

Il tipo di violazione verificatosi può influire sul livello di rischio presentato per le persone fisiche. Ad esempio, una violazione della riservatezza che ha portato alla divulgazione di informazioni mediche a soggetti non autorizzati può avere conseguenze diverse per una persona fisica rispetto a una violazione in cui tali informazioni mediche dell'Interessato siano state

erroneamente cancellati dal Titolare.

Natura, carattere sensibile e volume dei dati personali

Solitamente più i dati sono sensibili, maggiore è il rischio di danni per le persone interessate; occorre però tenere a mente che possono esservi diversi scenari, in concreto: è improbabile che la divulgazione del nome e dell'indirizzo di una persona fisica, in circostanze ordinarie, causi un danno sostanziale; tuttavia, se il nome e l'indirizzo di un genitore adottivo sono comunicati a un genitore biologico, le conseguenze potrebbero essere molto gravi tanto per il genitore adottivo quanto per il minore adottato.

Di norma una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale: violazioni relative a dati sulla salute, documenti di identità o dati finanziari come i dettagli di carte di credito, possono tutte causare danni di per sé, ma se tali dati fossero usati congiuntamente si potrebbe avere un'usurpazione d'identità.

Alcuni tipi di dati personali possono sembrare relativamente innocui, tuttavia occorre valutare attentamente ciò che questi dati possono rivelare sull'interessato: un elenco di clienti che accettano consegne regolari potrebbe non essere particolarmente sensibile, tuttavia gli stessi dati relativi a clienti che hanno richiesto l'interruzione delle loro consegne durante le loro vacanze potrebbero rappresentare un'informazione molto utile per la commissione di furti.

Analogamente, così come una piccola quantità di dati personali altamente sensibili può avere un impatto notevole su una persona fisica, lo stesso potrebbe valere per una vasta gamma di dati comuni, la quale può rivelare molte più informazioni su quella stessa persona. Inoltre, una violazione che interessa grandi quantità di dati personali relative a molte persone può avere ripercussioni su un numero corrispondentemente elevato di persone.

Facilità di identificazione delle persone fisiche

In caso di violazione della riservatezza, un fattore importante da considerare è la facilità con cui, accedendo ai dati compromessi, un soggetto possa riuscire a identificare persone specifiche o abbinare i dati con altre informazioni utili all'identificazione. A seconda delle circostanze, l'identificazione potrebbe essere possibile direttamente dai dati personali oggetto di violazione senza che sia necessaria alcuna ricerca speciale per scoprire l'identità dell'interessato, oppure potrebbe essere estremamente difficile, oppure possibile solo a determinate condizioni, abbinare i dati personali a una particolare persona fisica.

I dati personali protetti da un livello appropriato di cifratura saranno incomprensibili a persone non autorizzate che non dispongono della chiave di decifratura. Inoltre, anche una pseudonimizzazione opportunamente attuata può ridurre la probabilità che le persone fisiche vengano identificate in caso di violazione. Tuttavia, le tecniche di pseudonimizzazione da sole non possono essere considerate sufficienti a rendere i dati incomprensibili.

Caratteristiche

Una violazione può riguardare dati personali relativi a minori o ad altre

particolari dell'Interessato	persone fisiche vulnerabili, che possono di conseguenza essere soggette a un rischio più elevato di danno. Altri fattori concernenti la persona fisica potrebbero influire sul livello di impatto della violazione sulla stessa.
Numero di persone fisiche Interessate	Una violazione può riguardare solo una o poche persone fisiche oppure diverse migliaia di persone fisiche, se non molte di più. Di norma, maggiore è il numero di persone fisiche interessate, maggiore è l'impatto che una violazione può avere. Tuttavia, una violazione può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi.

3.1 - VALUTAZIONE DELLA GRAVITÀ E DELLA PROBABILITÀ

Per quanto attiene alla valutazione del possibile impatto sui diritti e le libertà degli interessati, il **TDB**, tenuto conto delle informazioni di cui sopra, ipotizza (in particolar modo sulla base delle informazioni di cui ai punti A.4, A.9 e A.11 della FASE 2) i danni che potrebbero derivare agli Interessati (a seconda della macro-tipologia di *Data Breach* intercorso) dall'accesso, dalla perdita e/o dalla modifica delle categorie di dati coinvolti, sulla base dell'elenco formulato dall'Autorità garante e qui riportato:

- ☐ Perdita del controllo dei dati personali
- ☐ Limitazione dei diritti
- ☐ Discriminazione
- ☐ Furto o usurpazione d'identità
- ☐ Frodi
- ☐ Perdite finanziarie
- ☐ Decifratura non autorizzata della pseudonimizzazione
- ☐ Pregiudizio alla reputazione
- ☐ Perdita di riservatezza dei dati personali protetti da segreto professionale
- ☐ Conoscenza da parte di terzi non autorizzati
- ☐ Qualsiasi altro danno economico o sociale significativo

La **GRAVITÀ** dei danni viene valutata[2] sulla base della tabella che segue:

TRASCURABILE	*Gli interessati non subiranno alcun impatto o potrebbero incontrare qualche inconveniente, superabile senza difficoltà*
BASSA	*Gli interessati potrebbero sperimentare inconvenienti significativi, superabili nonostante alcune difficoltà.*
MEDIA	*Gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative*
ALTA	*Gli interessati potrebbero sperimentare conseguenze significative, anche irrimediabili, che potrebbero non superare.*

[2] Ai fini della più corretta e completa valutazione, vengono in rilievo i principi di cui al successivo paragrafo "AVVERTENZA"

Il **TDB** procede dunque (in particolar modo sulla base delle informazioni di cui ai punti A.6, A.10 e A.12 della FASE 2) a valutare l'effettiva probabilità che tali danni si verifichino, giungendo infine ad individuare il grado di rischio complessivo, sulla base della tabella qui di seguito riportata.

In particolare, ai fini della valutazione, il **TDB** tiene conto dei seguenti aspetti (anche espressamente richiesti dall'Autorità garante in sede di eventuale notifica del *Data Breach*):

B.1) se la violazione ha comportato una perdita di riservatezza dei dati:

- ☐ i dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
- ☐ i dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
- ☐ i dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito

B.2) se la violazione ha comportato una modifica dei dati:

- ☐ i dati sono stati modificati e resi inconsistenti
- ☐ i dati sono stati modificati mantenendo la consistenza

B.3) se la violazione ha comportato la perdita di disponibilità dei dati, ciò ha determinato:

- ☐ il mancato accesso a servizi
- ☐ il malfunzionamento e difficoltà nell'utilizzo di servizi.

Ai fini del calcolo della probabilità, il **TDB** tiene altresì in considerazione le misure tecniche e organizzative adottate a seguito dell'evento per porre rimedio alla violazione e/o ridurne gli effetti negativi per gli interessati.

La **PROBABILITÀ** viene valutata sulla base della tabella che segue:

BASSA	*È improbabile che i danni si verifichino.*
MEDIA	*Ci sono ragionevoli probabilità che i danni si verifichino.*
ALTA	*È molto probabile che i danni si verifichino.*

Ai fini della valutazione in punto probabilità, è necessario tenere in considerazione che, alla luce di quanto indicato nelle Linee guida in materia di *Data Breach* (WP250rev.01), il verificarsi dei danni "*dovrebbe essere considerato probabile quando la violazione riguarda dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oppure che includono dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati*".

3.2 – VALUTAZIONE COMPLESSIVA DEL RISCHIO

Il **TDB** procede dunque alla valutazione complessiva del rischio, incrociando i due valori individuati al

paragrafo che precede, ovverosia il valore relativo alla GRAVITÀ e il valore relativo alla PROBABILITÀ, nella seguente matrice:

		GRAVITÀ			
		TRASCURABILE	BASSA	MEDIA	ALTA
PROBABILITÀ	BASSA				
	MEDIA				
	ALTA				

> Le celle contrassegnate dal segno di spunta () indicano che non è necessaria alcuna notifica all'Autorità o comunicazione agli interessati (da verificare tenendo conto delle caratteristiche del caso concreto).

> Le celle contrassegnate dal punto esclamativo su triangolo giallo () indicano la necessità di effettuare la notificazione all'Autorità garante per la protezione dei dati personali (cfr. *infra*, FASE 5).

> Le celle contrassegnate dal punto esclamativo su tondo rosso () indicano la necessità di effettuare sia la notificazione all'Autorità garante per la protezione dei dati personali, sia la **Comunicazione del *Data Breach* ai soggetti Interessati** (cfr. *infra*, FASE 5).

FASE 4: ADOZIONE DI MISURE DI SICUREZZA

Alla luce di quanto emerso nell'ambito delle valutazioni di cui ai paragrafi che precedono e tenuto altresì conto, in particolar modo, delle informazioni di cui ai punti A.4, A.5, A.6, A.7 e A.8 della FASE 2, il **TDB** individua le possibili misure di sicurezza, di carattere tecnico e/o organizzativo, che ritiene importante adottare ai fini di:

- porre rimedio alla violazione (ove possibile);
- ridurre gli effetti negativi che la violazione potrebbe avere nei confronti degli Interessati;
- prevenire il verificarsi di violazioni dello stesso tipo o similari.

Tenuto conto delle osservazioni degli altri membri, il SG dispone l'adozione delle misure di sicurezza che ritiene maggiormente adeguate per porre rimedio alla violazione o per ridurne gli effetti negativi. Nel fare ciò, il SG definisce le tempistiche entro cui le misure debbono essere implementate ed individua il Designato o i Designati a cui attribuire il compito e la responsabilità di tale implementazione.

ATTENZIONE: **tenuto conto delle caratteristiche del caso concreto, il SG può, d'urgenza, in qualunque FASE della presente Procedura, disporre senza formalità (anche oralmente) l'adozione o la modifica delle misure di sicurezza che ritiene urgenti e necessarie per porre rimedio alla violazione o per ridurne gli effetti negativi sugli Interessati.**

Tutte le decisioni così assunte e la relativa motivazione dovranno in ogni caso essere verbalizzate *prima o contestualmente* alla decisione di procedere o di non procedere alla notificazione della violazione all'Autorità garante per la protezione dei dati personali.

Successivamente all'implementazione di nuove misure di sicurezza è necessario provvedere, ove già svolte, ad effettuare nuovamente le valutazioni di cui alla FASE 3. Ove l'esito di dette valutazioni cambi in ragione delle misure di sicurezza implementate, nel verbale di cui *infra*, FASE 5, dovrà essere data evidenza del cambiamento, fornendo adeguate motivazioni.

FASE 5: NOTIFICAZIONI, COMUNICAZIONI E ALTRE ATTIVITÀ CONCLUSIVE

Entro lo scadere del sopra richiamato **termine di 72 ore**, all'esito delle analisi sino a qual momento condotte ed eventualmente rivalutata la probabilità sulla base delle misure di sicurezza aggiuntive (tecniche ed organizzative) sino a quel momento implementate, il **Segretario Generale**, sentito il parere degli altri membri del **TDB** ed in particolar modo del DPO, impiega la tabella di cui al par. 3.2 della presente Procedura[3] – qui di seguito riportata, per comodità – per fissare la valutazione complessiva del rischio.

		GRAVITÀ			
		TRASCURABILE	BASSA	MEDIA	ALTA
PROBABILITÀ	BASSA	✅	✅	⚠	❗
	MEDIA	✅	⚠	❗	❗
	ALTA	⚠	⚠	❗	❗

> Le celle contrassegnate dal segno di spunta (✅) indicano che non è necessaria alcuna notifica all'Autorità o comunicazione agli interessati (da verificare tenendo conto delle caratteristiche del caso concreto).

> Le celle contrassegnate dal punto esclamativo su triangolo giallo (⚠) indicano la necessità di effettuare la notifica all'Autorità garante per la protezione dei dati personali (cfr. *infra*, FASE 5).

> Le celle contrassegnate dal punto esclamativo su tondo rosso (❗) indicano la necessità di effettuare sia la notifica all'Autorità garante per la protezione dei dati personali, sia la **Comunicazione del *Data Breach* ai soggetti Interessati** (cfr. *infra*, FASE 5).

Il Segretario Generale procede dunque come segue.

A) **NEL CASO IN CUI LA VALUTAZIONE CORRISPONDA A** ✅ e si consideri, dunque, improbabile che la violazione presenti un rischio per i diritti e le libertà degli Interessati, il SG:

a.1) ove l'indagine conoscitiva di cui alla FASE 2 fosse ancora in corso, decide se:

prima opzione - quanto sino a quel momento emerso è sufficiente per considerare sufficientemente certa la valutazione di rischio;

seconda opzione - ritenere insufficienti le informazioni sino a quel momento raccolte ai fini della valutazione del rischio; in tal caso, sentito il parere del DPO, decide se procedere senza notificazione, ovvero se effettuare comunque la notificazione di avvenuto *Data Breach* all'Autorità garante per la protezione dei dati personali (secondo le modalità indicate nel prosieguo della presente Procedura), riservando integrazioni una volta ultimata la raccolta e l'analisi delle informazioni;

---------- **[SCADENZA DEL TERMINE DI 72 ORE]** ----------

a.2) con il supporto del **TDB**, valuta se vi sono ragioni di opportunità e di tutela che suggeriscono (anche se non necessaria) di effettuare la comunicazione del *Data Breach* agli Interessati (cfr. par. "COMUNICAZIONE AI SOGGETTI INTERESSATI"); se decide di procedere con tale comunicazione, ne dà immediato avviso al Presidente;

[3] Fatto salvo quanto previsto dal paragrafo "AVVERTENZA".

a.3) chiude il verbale relativo agli esiti di tutte le FASI, allegando il parere formale del DPO.

a.4) provvede ad aggiornare il Registro dei *Data Breach*, come da *format* allegato e provvede altresì, alla prima occasione utile, a riferire dell'accaduto alla Giunta camerale.

B) **NEL CASO IN CUI LA VALUTAZIONE CORRISPONDA A**  e, dunque, risulti che la violazione possa comportare un rischio per i diritti e le libertà degli interessati, il SG:

b.1) su delega del Presidente (legale rappresentante *pro tempore*) della CCIAA DI PAVIA, procede senza indugio alla compilazione, alla sottoscrizione e all'inoltro della notificazione di *Data Breach* all'Autorità garante per la protezione dei dati personali (secondo le modalità indicate ne prosieguo della presente Procedura), riservandosi di integrare la segnalazione ove l'indagine conoscitiva di cui alla FASE 2 fosse ancora in corso;

- **[SCADENZA DEL TERMINE DI 72 ORE]** -

b.2) informa senza ritardo il Presidente dell'avvenuta notifica e lo tiene aggiornato in relazione ad ogni ulteriore sviluppo;

b.3) con il supporto del **TDB**, valuta se vi sono ragioni di opportunità e di tutela che suggeriscono (anche se non necessaria) di effettuare la comunicazione del *Data Breach* agli Interessati (cfr. par. "COMUNICAZIONE AI SOGGETTI INTERESSATI"); se decide di procedere con tale comunicazione, ne dà immediato avviso al Presidente;

b.4) verifica se vi sono altre misure, rispetto a quelle già adottate, che possono essere implementate nel breve, medio o lungo periodo e, se del caso, redige il relativo piano d'azione;

b.5) chiude il verbale relativo agli esiti di tutte le FASI, allegando il parere formale del DPO e copia della notificazione;

b.6) provvede ad aggiornare il Registro dei *Data Breach*, come da format allegato e provvede a riferire dell'accaduto, alla prima occasione utile, alla Giunta camerale.

C) **NEL CASO IN CUI LA VALUTAZIONE CORRISPONDA A**  e, dunque, risulti che la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il SG:

c.1) su delega del Presidente (legale rappresentante pro tempore) della CCIAA DI PAVIA, procede senza indugio alla compilazione, alla sottoscrizione e all'inoltro della notificazione di *Data Breach* all'Autorità garante per la protezione dei dati personali (secondo le modalità indicate ne prosieguo della presente Procedura), riservandosi di integrare la segnalazione ove l'indagine conoscitiva di cui alla FASE 2 fosse ancora in corso;

- **[SCADENZA DEL TERMINE DI 72 ORE]** -

c.2) effettua la comunicazione del *Data Breach* agli Interessati (cfr. par. "COMUNICAZIONE AI SOGGETTI INTERESSATI"); **NB: tale comunicazione, se ve ne è il tempo, è possibile effettuarla anche *prima* della notifica all'Autorità garante**;

c.3) informa senza ritardo il Presidente delle avvenute notifica e comunicazione di cui ai punti che precedono, mantenendolo aggiornato in relazione ad ogni ulteriore sviluppo;

c.4) verifica se vi sono altre misure, rispetto a quelle già adottate, che possono essere implementate nel breve, medio o lungo periodo e, se del caso, redige il relativo piano d'azione;

c.5) chiude il verbale relativo agli esiti di tutte le FASI, allegando il parere formale dal DPO e copia della notificazione;

c.6) provvede ad aggiornare il Registro dei *Data Breach*, come da format allegato e provvede a riferire dell'accaduto, alla prima occasione utile, alla Giunta camerale.

NOTIFICAZIONE DEL DATA BREACH ALL'AUTORITÀ DI CONTROLLO

Con il provvedimento n° 209 del 27 maggio 2021, l'Autorità garante per la protezione dei dati personali ha stabilito una nuova procedura per la notificazione telematica delle violazioni dei dati personali.

È importante notare che **tale procedura telematica costituisce oggi l'unica ed ordinaria modalità** mediante cui l'Autorità garante acquisisce la notifiche.

Detta procedura prevede che sia una persona fisica ad effettuare e sottoscrivere la notifica, per conto del Titolare del trattamento. È previsto che tale persona fisica non solo agisca in nome e per conto del Titolare, ma si assuma altresì la responsabilità in relazione al contenuto della notifica, ai sensi dell'art. 168 D.Lgs. 196/2003[4]. Per tali ragioni, il soggetto che effettua la notifica deve necessariamente essere il legale rappresentante del Titolare o un'altra persona che agisce su delega dello stesso.

Nell'ambito della presente Procedura, il soggetto che provvede a compilare, inoltrare e sottoscrivere la notifica, è individuato nel SG, su delega (generale, ovvero speciale caso per caso) del Presidente della CCIAA DI PAVIA.

Il **link diretto** per poter compilare ed inoltrare la notifica all'Autorità garante per la protezione dei dati personali è il seguente:

https://servizi.gpdp.it/databreach/s/scelta-auth

Nel caso in cui il link diretto sopra riportato non fosse più attivo, è possibile accedere alla pagina di notifica per il tramite del portale https://servizi.gpdp.it/databreach, oppure cercando la relativa voce collegandosi al sito internet dell'Autorità garante, raggiungibile agli indirizzi https://www.garanteprivacy.it e https://www.gpdp.it

Durante la compilazione della "prima notifica", il SG deve indicare se trattasi di una notifica "preliminare" o di una notifica "completa". Tale qualificazione ha esclusivamente la funzione di discriminare

[4] Art. 168 Codice Privacy (*Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*): "[1] *Salvo che il fatto costituisca piu' grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, e' punito con la reclusione da sei mesi a tre anni.* [2] *Fuori dei casi di cui al comma 1, e' punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarita' di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti*".

l'applicazione dei controlli che garantiscono la presenza del *set* "minimo" di informazioni che il titolare è tenuto a fornire: a titolo esemplificativo, una notifica in cui il Titolare non fornisca informazioni salienti, quali le categorie di dati personali coinvolti, le possibili conseguenze per gli interessati, ecc., non può essere qualificabile come "completa" in quanto priva degli elementi essenziali. Il SG ha sempre la facoltà di qualificare una notifica come "preliminare" qualora ritenga di dover integrare successivamente le informazioni fornite, pur avendo già fornito gli elementi essenziali.

Durante la compilazione di alcune **sezioni è possibile indicare la volontà di allegare un file contenente ulteriori informazioni di dettaglio**. Sono accettati esclusivamente allegati in formato *.pdf di dimensioni inferiori ai 2,5 MB.

COMUNICAZIONE DEL DATA BREACH AGLI INTERESSATI

Ai sensi dell'art. 34, par. 1 GDPR, quando il *Data Breach* è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento deve comunicare all'Interessato l'avvenuta violazione. Tale comunicazione, precisa la norma, deve essere effettuata ***"senza ingiustificato ritardo"***[5].

Ove la violazione non ricada nei casi individuati a mezzo della tabella[6] di cui *supra*, par. 3.2, si suggerisce di valutare se sussistono comunque ragioni di opportunità che suggeriscono l'inoltro della comunicazione agli Interessati. Nel compiere questa valutazione, occorre tenere a mente, da un lato, che gli Interessati vanno protetti anche da inutili disturbi che potrebbe arrecare la comunicazione stessa e, dall'altro lato, (come precisato dal Considerando 88 del GDPR) che una divulgazione prematura della violazione potrebbe in alcuni casi "*ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali*". Ove sorgano dubbi sull'opportunità o meno di contattare gli Interessati, le Linee guida WP 250rev.01 hanno chiarito che il Titolare può consultarsi con l'Autorità garante.

Nell'ambito della comunicazione all'Interessato è necessario fornire (almeno) le seguenti informazioni:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del DPO;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

A seconda della natura della violazione, il Titolare del trattamento dovrebbe anche fornire indicazioni specifiche agli Interessati in relazione alle modalità con cui loro stessi possano proteggersi dalle possibili conseguenze negative della violazione.

La comunicazione di *Data Breach* deve essere inoltrata direttamente agli Interessati coinvolti. A seconda delle circostanze, ciò potrebbe significare che il Titolare del trattamento debba utilizzare diversi metodi di

[5] Quanto alla tempestività della comunicazione, il Considerando 86 del GDPR precisa che le comunicazioni agli Interessati "*dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione*".

[6] Fatto salvo quanto previsto dal paragrafo "AVVERTENZA".

comunicazione, anziché un singolo canale di contatto. Ove la comunicazione diretta a ciascun Interessato richieda uno sforzo sproporzionato, occorre procedere con una **comunicazione pubblica** o con altra misura similare, che permetta di informare gli interessati con analoga efficacia. Nel comunicare una violazione agli interessati si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi *standard*. Ciò contribuisce a rendere la comunicazione del *Data Breach* **chiara e trasparente**. Ove sorgano dubbi sulle modalità con cui contattare gli Interessati, le Linee guida WP 250rev.01 hanno chiarito che il Titolare può consultarsi con l'Autorità garante.

TENUTA DEL REGISTRO DATA BREACH

Indipendentemente dal fatto che una violazione debba o meno essere notificata all'Autorità garante o comunicata agli Interessati, il GDPR (art. 33, par. 5) prevede che, ai sensi del principio di *accountability*, il Titolare documenti "*qualsiasi violazione dei dati, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio"*. L'Autorità di controllo può in qualunque momento richiedere di consultare tali registrazioni.

Per tale ragione, è importante che a seguito di ogni violazione venga compilato e tenuto aggiornato il Registro allegato alla presente Procedura.

Il GDPR non specifica un periodo di conservazione di tale Registro. Se il Registro *Data Breach* non contiene dati personali, il principio di limitazione della conservazione previsto dal regolamento non si applica e, pertanto, tale Registro può essere conservato per un periodo di tempo illimitato. Ove, invece, nel Registro vengano inseriti dati di carattere personale (es. le generalità del segnalante o del soggetto Interessato i cui dati sono stati violati), è necessario procedere all'individuazione del tempo di *data retention* e della più opportuna base giuridica legittimante il trattamento, fornendone indicazione anche nel Registro delle attività di trattamento, nonché fornendo apposita informativa (ove possibile) a tutti i soggetti i cui dati vengono trattati nell'ambito del Registro *Data Breach*. In generale, il periodo di conservazione del Registro *Data Breach* deve tenere conto del fatto che la CCIAA DI PAVIA può essere chiamata a fornire prove all'Autorità di controllo in merito al rispetto della summenzionata norma e del principio di *accountability*.

Il Registro allegato alla presente procedura è annotabile mediante schede composte da nr. 2 (due) pagine ciascuna. Alla scheda del Registro relativa a ciascuna violazione, il SG dovrà allegare il verbale o i verbali redatti nel corso della valutazione e della gestione del *Data Breach*. Le Linee guida WP 250rev.01 raccomandano infatti di "*documentare anche il ragionamento alla base delle decisioni prese in risposta a una violazione. In particolare, se una violazione non viene notificata, è opportuno documentare una giustificazione di tale decisione. La giustificazione dovrebbe includere i motivi per cui il titolare del trattamento ritiene improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche*".

ATTENZIONE: la mancata corretta documentazione dei *Data Breach* può comportare l'esercizio da parte dell'Autorità garante dei suoi poteri ai sensi dell'art. 58 GDPR e l'imposizione di una sanzione amministrativa pecuniaria ai sensi dell'art. 83 GDPR.

È importante indicare immediatamente, all'apertura di una nuova scheda, in alto a sinistra, il numero progressivo di scheda / annotazione (es. "**001**" o "**01-2021**"). Tale numero va riportato, identico, su entrambe le pagine della scheda. Quando si registrano per la prima volta i fatti relativi ad una specifica violazione e, dunque, viene effettuata una nuova annotazione sul Registro, occorre flaggare la voce "Nuovo evento". Ove, in una data successiva, emerga la necessità di integrare o modificare le informazioni su uno specifico evento, già annotato nel Registro, sarà possibile aprire una nuova scheda,

indicando che la stessa è integrativa rispetto alla scheda nr. ##; in calce alla scheda precedente sarà inoltre possibile flaggare la voce (in calce) "*Questa scheda è stata integrata e/o modificata dalla successiva nr. ……."*, compilando l'apposito campo.

ATTIVITÀ ULTERIORI E SUCCESSIVE

Ove si sospetti che la violazione sia stata provocata in maniera intenzionale da uno o più soggetti interni ovvero esterni alla CCIAA DI PAVIA, il SG, con il supporto del **TDB**, avvia un parallelo processo di raccolta delle evidenze o prove, disponendo ulteriori investigazioni, anche difensive.

Tale attività, ove necessario, può essere gestita secondo quanto previsto, a seconda dei casi, dall'art. 391-*nonies* o dall'art. 327-*bis* c.p.p. e deve rispettare gli *standard* e le normative in termini di analisi forense, al fine di poter intraprendere successivamente le più opportune azioni legali nei confronti degli eventuali responsabili.

In generale, all'esito delle notificazioni all'Autorità garante a agli interessati, il DPO deve:

- gestire in prima persona le relazioni con l'Autorità garante per la protezione dei dati personali;
- coordinare la gestione delle istanze e delle richieste di informazioni pervenute alla CCIAA DI PAVIA dagli Interessati in relazione al *Data Breach* intercorso.

RIESAME ED AGGIORNAMENTO DELLA PRESENTE PROCEDURA

Nell'ottica del miglioramento continuo e del raggiungimento degli obiettivi di *compliance* alla normativa di riferimento, anche al fine di garantire che l'efficacia delle misure tecniche e organizzative implementate sia "*testata regolarmente*" (art. 32, par. 1, lett. d), del GDPR), la presente Procedura dovrà essere sottoposta a riesame / aggiornamento, almeno in occasione:

- dell'emanazione di nuove disposizioni normative, Linee guida, pronunce giurisprudenziali, provvedimenti dell'Autorità garante per la protezione dei dati personali, di carattere cogente e/o interpretativo che impattino sulla disciplina del *Data Breach*;
- di cambiamenti significativi del Modello organizzativo *privacy* della CCIAA DI PAVIA;
- nel caso di applicazione di sanzioni da parte delle Autorità di controllo.

Necessità di riesame possono essere segnalate dai Designati e sono valutate dal SG in collaborazione con il DPO.