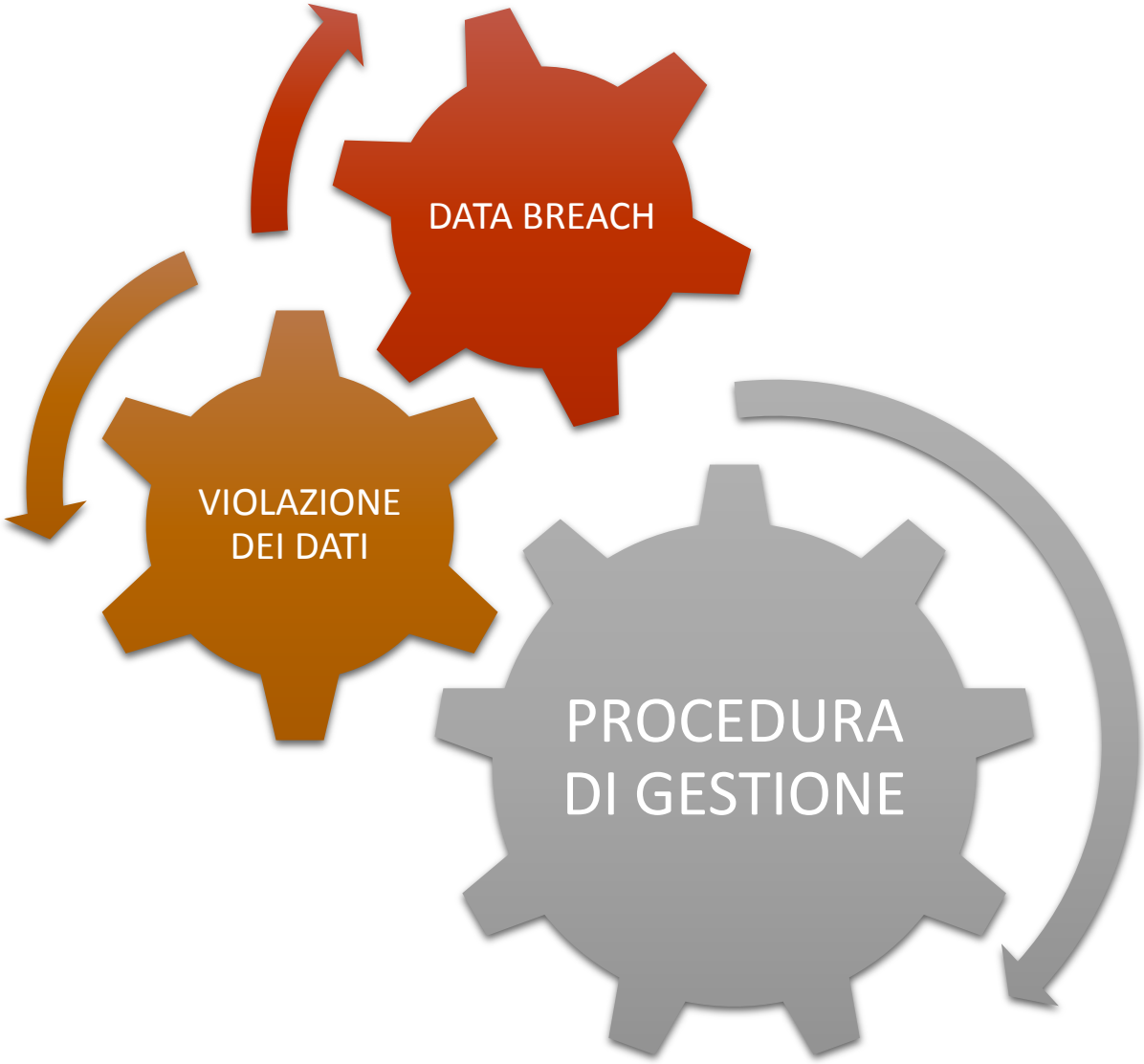


Titolo	Procedura di gestione delle violazioni di dati personali		
Autore	Liceo delle Scienze Umane "Contessa Tornielli Bellini" - Novara		
Data di emissione	03/08/2020	Versione	01

Sommario

I. INTRODUZIONE

GLOSSARIO

- **Violazione dei dati personali o *Data Breach***- è 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 personali trasmessi, conservati o comunque trattati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.
- **GDPR** - Regolamento (UE) 2016/679 in materia di protezione dei dati personali, nonché della libera circolazione di tali dati, che abroga la direttiva 95/46/CE sulla stessa materia. Pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04/05/2016, entrato in vigore il 24/05/2016 e definitivamente applicabile in via diretta in tutti i paesi UE dal 25/05/2018. L'acronimo GDPR si riferisce al termine anglosassone "General Data Protection Regulation", mentre l'acronimo RGPD si riferisce alla definizione nazionale "Regolamento Generale sulla Protezione dei Dati".
- **CodicePrivacy**- Codice nazionale in materia di protezione dei dati personali - D. Lgs 30 giugno 2003 n. 196, modificato dal D.Lgs. 10 agosto 2018 n. 101.
- **Garante** - Garante per la Protezione dei Dati Personali, istituito dalla Legge 31 dicembre 1996 n. 675, quale autorità amministrativa pubblica di controllo indipendente; il GDPR identifica questa figura denominandola "Autorità di controllo" (V. artt. 51 e ss. del GDPR).
- **Titolare del trattamento** – Titolare del trattamento è 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.
- **Responsabile del trattamento dei dati** – Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta i dati per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR)
- **Accountability** - principio per cui il Titolare deve dimostrare l'adozione di politiche privacy e misure di sicurezza adeguate a prevenire il rischio di *Data Breach*, in conformità al GDPR.
- **Privacy by design** – principio che prevede l'adozione di misure di sicurezza tecniche ed organizzative, non solo nel momento dell'esecuzione, ma sin dalla progettazione di un'attività che comporta il trattamento di dati personali.
- **Privacy by default** – principio secondo cui, per impostazione predefinita, il titolare può trattare solo i dati personali nella misura necessaria e sufficiente per le finalità prestabilite e per il periodo strettamente necessario a raggiungerle.
- **RACI** – È la matrice di assegnazione responsabilità, che pone in relazione le risorse umane con le attività delle quali sono responsabili, o con loro aggregazioni. Tipicamente, pone in relazione le risorse umane di un organigramma con i principali processi aziendali dei quali sono responsabili, oppure, a livello più basso, con le attività previste dal processo aziendale. La matrice RACI, dunque, specifica il tipo di relazione fra la risorsa e l'attività: *Responsible, Accountable, Consulted, Informed*. Con tale strumento viene indicato "chi fa che cosa", all'interno di una organizzazione.
- **WP29–** gruppo di lavoro indipendente,istituito in virtù dell'art. n. 29 della direttiva 95/45/CE; ha funzioni consultive dell'UE, nell'ambito dalla protezione dei dati personali e della vita privata; oggi sostituito dall'EDPB (*European Data Protection Board*)
- **EDPB** – acronimo di *European Data Protection Board***;** Il Comitato Europeo Per La Protezione Dei Dati è un organo europeo indipendente, che contribuisce all'applicazione delle norme sulla protezione dei dati uniformemente in tutta l'Unione Europea e promuove la cooperazione tra le autorità competenti per la protezione dei dati dell'UE. Il Comitato Europeo Per La Protezione Dei Dati è composto da

rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati (GEPD).

DEFINIZIONE DI DATA BREACH E RIASSUNTO DEI PRINCIPALI ADEMPIMENTI

Per ***Data Breach*** si intende un evento la cui conseguenza comporta una **violazione dei dati personali**.

Più nello specifico, è un **incidente di sicurezza che va ad inficiare la riservatezza, l'integrità e la disponibilità dei dati personali**, causando, accidentalmente o volontariamente, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso illecito ai dati personali trasmessi, conservati o comunque trattati (art. 4, n. 12, GDPR e art. 32 par. 1 GDPR).

Da tali eventi, può sorgere il **rischio di danni per i diritti e le libertà delle persone fisiche** i cui dati siano stati violati.

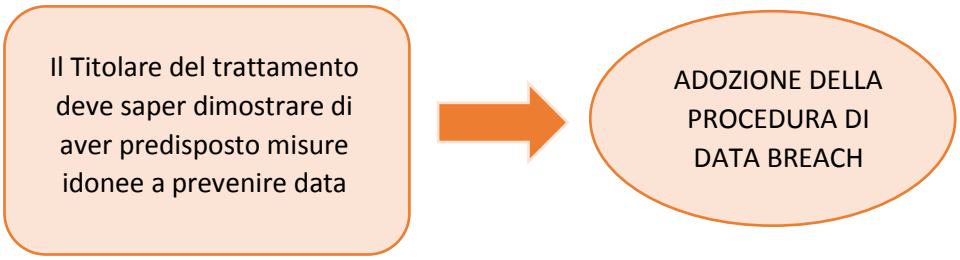
Un *Data Breach*può avere origine sia dall'esterno, sia dall'interno della struttura del titolare.

Sono, **ad esempio**, potenziali cause di violazioni dei dati personali:

- ✓ la modificazione erronea di un database
- ✓ un malware che impedisce l'apertura di una cartella sul server,
- ✓ lo smarrimento di una chiavetta USB, di un telefonino aziendale,
- ✓ l'invio di un dato personale ad un terzo non autorizzato.

È importante aver presente che, in generale, il titolare deve mettere in atto, ed essere in grado di dimostrare, di aver adottato misure tecniche ed organizzative adeguate a garantire che il trattamento è effettuato in conformità del Regolamento Europeo (art. 24 paragrafo n. 1 del GDPR).

Quest'obbligo si sostanzia anche nella procedura che il titolare deve seguire in caso di violazione dei dati personali (*Data Breach*), che, qui di seguito, viene schematicamente illustrata. Tale procedura verrà poi esplicata più dettagliatamente nel proseguo del presente documento



SCHEMA DELLA PROCEDURA DI DATA BREACH

L'art. 33 GDPR impone al titolare, che abbia ricevuto una segnalazione di *Data Breach*, di **valutare** sela violazione dei dati personali presenti **rischi per i diritti e le libertà delle persone** fisiche.

Per la gestione del processo di *Data Breach*, il titolare deve avvalersi della struttura che lo compone ed eventualmente dei soggetti nominati responsabili del trattamento ai sensi dell'art.28 GDPR.

Qualora il titolare riscontri un **rischio probabile**, ha l'obbligo di **notificare all'Autorità di controllo** (Garante per la Protezione dei Dati Personali) la violazione dei dati personali **entro le 72 ore** dal momento in cui ne è venuto a conoscenza (paragrafo n. 1). Tale termine non è perentorio, tuttavia nel caso in cui esso sia superato, unitamente alla notifica, occorre **giustificare i motivi del ritardo** (art. 33 paragrafo n. 1 del GDPR). La **finalità** di questa regola è quella di **evitare l'insorgenza o l'aggravamento di danni** alle persone interessate (perdita di controllo dei dati, limitazione dei diritti dell'interessato, discriminazione, furto o usurpazione dell'identità, perdite finanziarie, ecc.).

Si precisa che l'incidente di sicurezza informatico va segnalato anche al "Computer Security Incident Response Team – Italia" (CSIRT), qualora non si tratti di vulnerabilità già note a tale ente e da esso quindi già catalogate (https://csirt.gov.it/segnalazione).

Il mancato rispetto dell'obbligo di notificatone l'Autorità di Controllo nella condizione di applicare le **misure correttive** a sua disposizione:

- avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati (poteri previsti dall'art. 58 GDPR);
- **sanzioni** amministrative, il cui importo, secondo l'art. 83 GDPR, può arrivare a 10.000.000 € o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

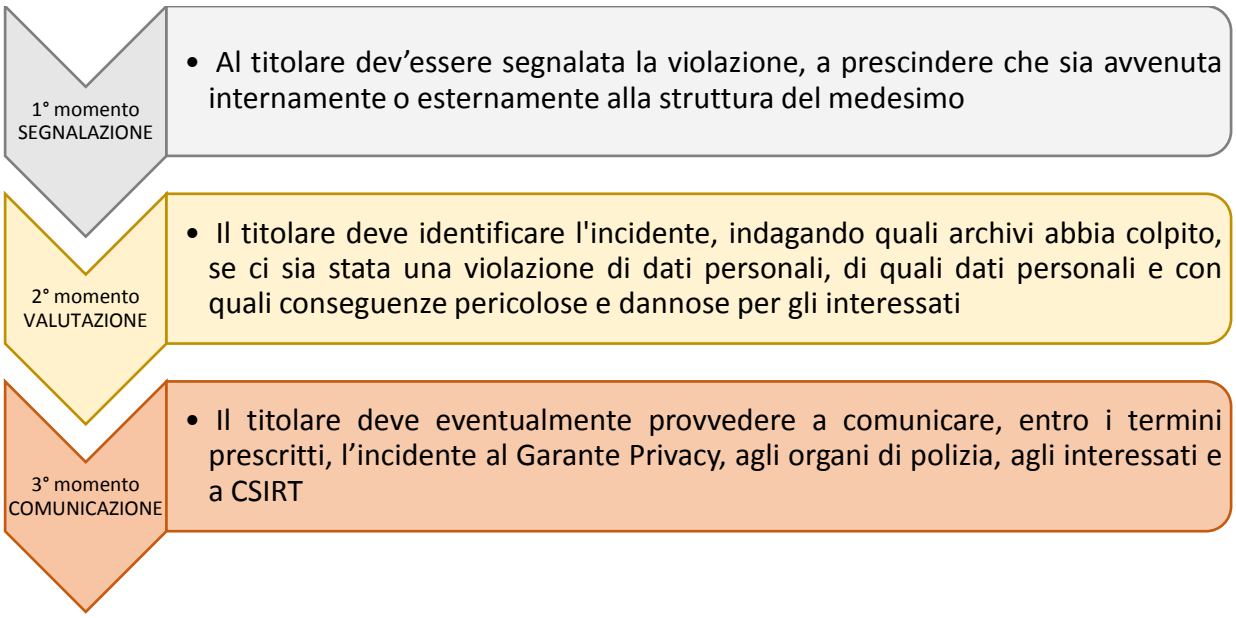
La mancata notifica può inoltre dare luogo successivi accertamenti da parte del Garante, rappresentando invero un indizio di carenze strutturali più profonde che, se riscontrate, comporterebbero potenzialmente l'irrogazione di ulteriori sanzioni.

Inoltre, quando la violazione dei dati è suscettibile di presentare **rischio elevato** per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve, senza ingiustificato ritardo, **comunicare all'interessato** la violazione (art. 33 paragrafo n. 1 del GDPR).

Tutti gli eventi di *Data Breach* (compresi quelli per cui non sono necessarie le notifiche), le circostanze, le conseguenze e i rimedi adottati dal titolare, devono essere documentati dal titolare su un **registro** (art. 33 par. 5 del GDPR), tenuto secondo le indicazioni fornite dal Garante con il provvedimento n. 393 del 02/07/2015 (GU n. 179 del 04/08/2015 - doc. web n. 4129029).

II. FASI DEL PROCESSO DI *Data Breach*

La procedura di *Data Breach* si basa su tre momenti:

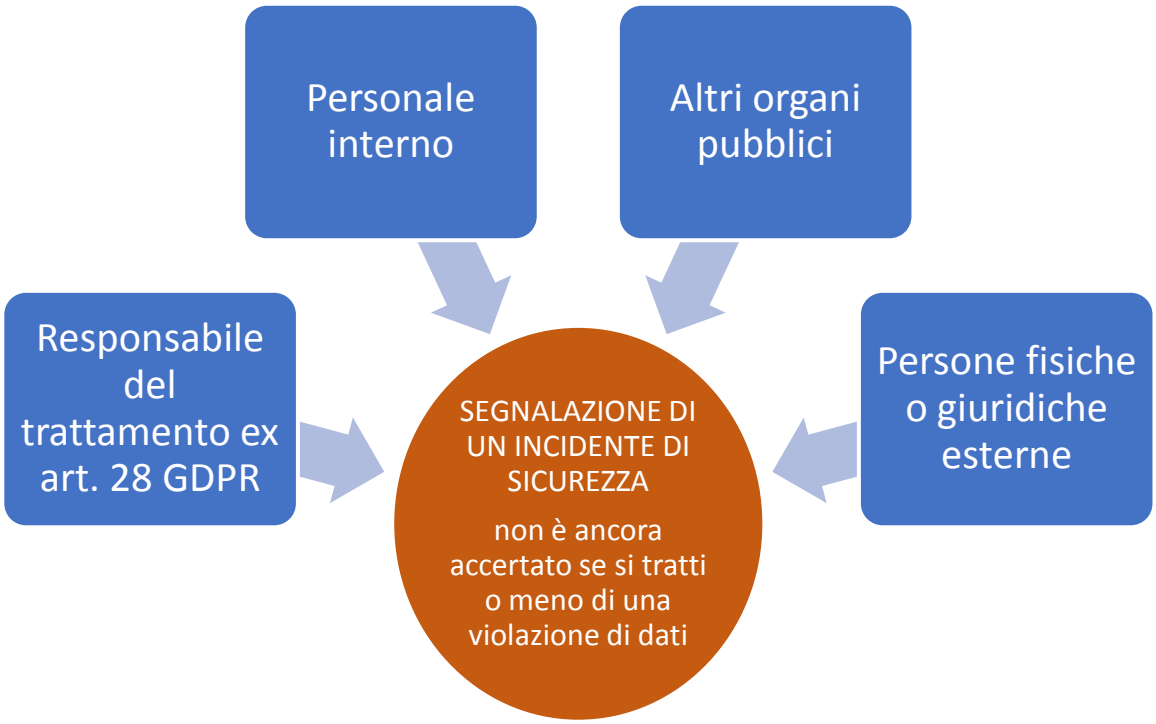


La procedura di *Data Breach* si divide a sua volta in più fasi dettagliate:

1° momento	**ACQUISIZIONE** Fase 1	Rilevazione e comunicazione dell'evento al Titolare
2° momento	**GESTIONE TECNICA** Fase n. 2	Raccolta informazioni; definizione dei soggetti coinvolti; Accertamento dell'effettiva sussistenza del *Data Breach*; analisi del tipo di violazione
2° momento	**VALUTAZIONE** Fase n. 3	Occorre valutare se l'incidente abbia provocato una violazione di dati da cui siano derivati rischi per i diritti delle persone fisiche
3° momento	**NOTIFICA AL GARANTE** Fase n. 4	Se dalla violazione dei dati deriva un rischio probabile per i diritti e le libertà degli interessati.
3° momento	**SEGNALAZIONE AGLI ORGANI DIPOLIZIA** Fase n. 5	Se dalla violazione dei dati deriva un rischio elevato per i diritti e le libertà degli interessati
3° momento	**COMUNICAZIONE AGLI INTERESSATI** Fase n. 6	Comunicazione agli interessati e raccolta riscontri dell'avvenuta comunicazione

REGISTRO DEGLI INCIDENTI E DELLE VIOLAZIONI
Il titolare deve tenere un registro dove documentare, anche da un punto di vista temporale, tutti gli incidenti subìti, descrivendo se da essi sia derivata una violazione di dati personali e motivando quali azioni abbia conseguentemente deciso di intraprendere.

FASE N. 1 – ACQUISIZIONE (1° momento)



La prima fase nella gestione del *Data Breach* **è costituita dalla comunicazione dell'incidente di sicurezza e/o presunta violazione al titolare**.

Comunicazione e raccolta della segnalazione

La comunicazione dev'essere effettuata, ove possibile, in forma scritta, anche utilizzando mezzi elettronici (es. posta elettronica), nel rispetto delle seguenti prescrizioni:

1. predisporre la segnalazione in modo tale che sia **più completa e dettagliata possibile**, mai omettendo di indicare le modalità con cui il segnalante ha preso consapevolezza della violazione; le informazioni che possono essere riportate sono le seguenti: identificazione dei segnalanti, con indicazione dei loro dati di contatto (indirizzo di reperibilità, numeri telefonici, indirizzo di posta elettronica),data ed ora in cui la segnalazione è avvenuta, descrizione dell'incidente di sicurezza e dei dati ipoteticamente violati, ecc.;
2. individuare i precisi **riferimenti temporali** (data ed ora) di quando la segnalazione è stata inoltrata al titolare e da questi acquisita; da tale momento decorrono, infatti, **le 72 ore per l'eventuale notifica al Garante che dev'essere effettuata dal titolare**;
3. **anche le segnalazioni anonime e/o orali** devono essere inviate e acquisite per consentire al titolare di accertare la reale sussistenza della violazione, disporre l'eventuale notifica o le comunicazioni ed assumere i provvedimenti atti ad evitare l'aggravamento della situazione.
4. la comunicazione al titolare deve essergli comunque inoltrata, **anche qualora vi sia il dubbio che l'incidente non abbia davvero comportato una violazione dei dati personali**; sarà infatti poi il titolare stesso - eseguita la valutazione sulla base di quanto emerso nella successiva fase n. 2 - a stabilire se ci si trovi o meno davanti ad un caso di violazione di dati;
5. **il segnalante deve mettersi a completa disposizione del titolare**, per consentirgli di eventualmente integrare le informazioni.

Schema tipo di comunicazione al titolare

L'**Allegato n. 1** rappresenta uno schema che può essere utilizzato per la comunicazione al Titolare di una violazione (reale o presunta), del quale è consigliato l'utilizzo.

Tale schema, insieme alla presente procedura e all'Allegato 2, sono reperibili presso il server della sede amministrativa di Baluardo La Marmora, 10, nella cartella denominata "PRIVACY".

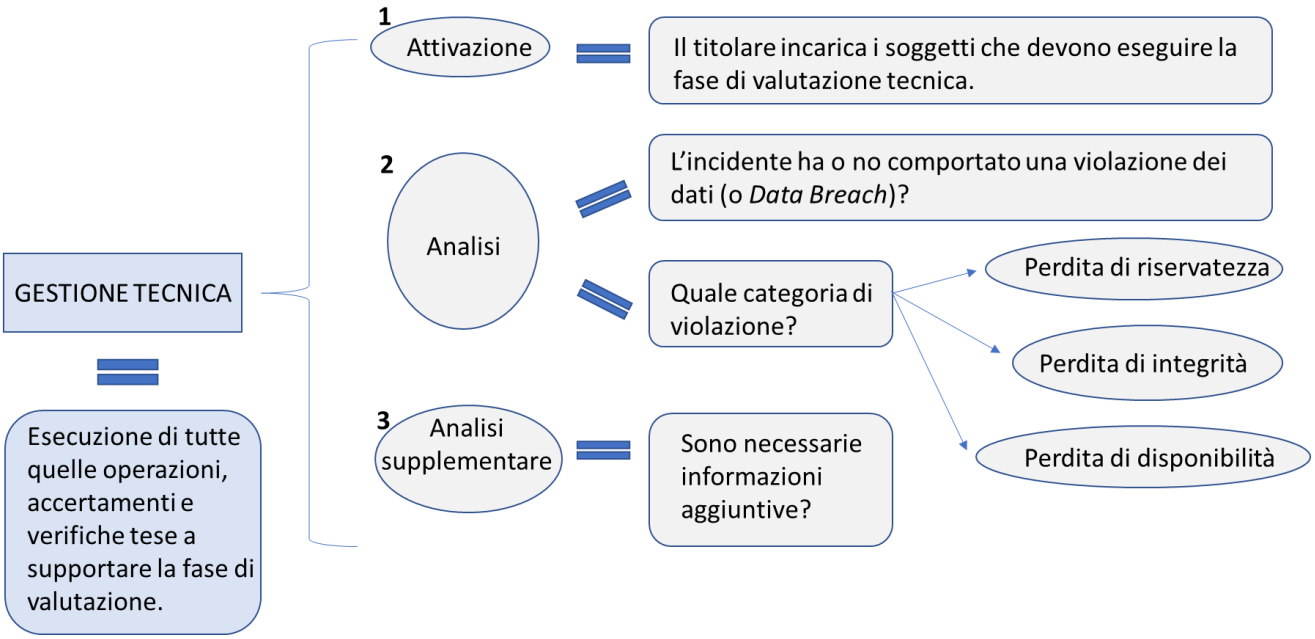
AZIONI OPERATIVE

1) Il modulo di segnalazione (Allegato n. 1) viene messo a disposizione presso il server della sede amministrativa di Baluardo La Marmora, 10
2) Una volta compilato il modulo, è da consegnare a mano presso la stessa sede oppure si può inviare con oggetto "**SEGNALAZIONE VIOLAZIONE**" tramite:

   E-mail: nopm010005@istruzione.it

   PEC: nopm010005@pec.istruzione.it
3) La comunicazione dev'essere effettiva. Ciò significa che, contestualmente a quella scritta è necessario avvisare telefonicamente la segreteria al numero 0321 - 627125

FASE N. 2 – GESTIONE TECNICA (2° momento)



Per gestione tecnica s'intende **l'esecuzione di tutte quelle operazioni, accertamenti e verifiche tese a supportare la fase di valutazione**.

Questa fase dovrebbe concludersi nel più breve tempo possibile (circa dieci ore),per consentire al titolare il primo processo decisionale di valutazione e permettergli di eseguire le eventuali notifiche e comunicazioni entro i termini previsti

L'art. 33, paragrafo n. 4, del GDPR recita: "**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". Coerentemente, il WP29, nelle sue linee guida, chiarisce che il Regolamento Europeo ammette che i titolari possano non aver sempre a disposizione tutte le informazioni relative ad una violazione entro il termine delle settantadue ore, in quanto i dettagli dell'incidente potrebbero non essere completamente disponibili in questo breve lasso temporale, necessitando di ulteriori indagini ed approfondimenti.

La fase potrebbe articolarsi in:

A. ATTIVAZIONE

Il titolare (o suo sostituto o delegato), venuto a conoscenza della violazione, incarica gli organi apicali ed eventualmente i responsabili del trattamento ex art. 28 GDPR ad eseguire la fase di valutazione tecnica. Il titolare si avvale dei responsabili ex art. 28 GDPR qualora la violazione si sia verificata, in tutto od in parte, in operazioni di trattamento svolte da questi ultimi per conto del titolare e sia ritenuto comunque utile il loro contributo (ad es. quando siano i fornitori di servizi di connettività).

B. ANALISI

Analisi preliminare

Preliminarmente, occorre appurare **se l'incidente segnalato abbia causato o meno una violazione di dati (*Data Breach*)**.

In ogni caso, un primo giudizio di inaffidabilità del segnalante non è idoneo di per sé a determinare la chiusura del processo, poiché occorrerà comunque appurare se la violazione si sia effettivamente verificata.

Tutte le segnalazioni, comprese quelle non veritiere che comportano la chiusura anticipata della fase di gestione tecnica, devono essere documentate nel **registro degli incidenti** tenuto dal titolare.

Analisi della tipologia di violazione dei dati: perdita riservatezza dei dati/ perdita integrità dei dati/ perdita disponibilità dei dati

Occorre ora individuare **a quale categoria la violazione possa appartenere** fra quelle identificate dal WP29, tenendo comunque conto che essa potrebbe riferirsi anche a più categorie:

a) **Violazione di riservatezza**: tale violazione si verifica per una divulgazione o un accesso ai dati non autorizzato, volontario o accidentale.
   Questo tipo di violazione può manifestarsi in diversi modi; a puro titolo di esempio:
   - quando vengono inoltrati erroneamente messaggi contenenti dati personali a soggetti terzi e non destinatari dei medesimi;
   - quando un operatore abbandona la propria postazione di lavoro senza prima prendere le opportune precauzioni (riordinare la documentazione, lasciare attive procedure sulla risorsa informatica utilizzata, ecc.) e terze persone conseguentemente prendono visione di informazioni private;
   - quando un soggetto, in malafede e senza esserne autorizzato, comunica dei dati non pubblici a terzi.

b) **Violazione di integrità**: tale violazione si verifica per un'alterazione di dati personali.
   Un'alterazione accidentale si può verificare per errore umano (ad es. nel momento di un aggiornamento delle informazioni), per un disguido tecnico quando all'interno di una base dati si perdono i collegamenti a determinate informazioni (integrità referenziale).
   Un'alterazione non autorizzata può essere la conseguenza di un attacco esterno o di una manipolazione inconsapevole da parte di personale non competente.

c) **Violazione di disponibilità**: tale violazione si verifica per la perdita, l'inaccessibilità, o la distruzione dei dati personali, accidentale o non autorizzata.
   La casistica è molto ampia; il WP29, nelle sue linee guida, riporta i seguenti esempi:
   - i dati sono cancellati accidentalmente o da soggetti non autorizzati;
   - la chiave di decriptazione viene persa;
   - i dati vengono persi dall'ambiente di produzione e non possano essere ripristinati integralmente dalle copie di sicurezza, con la conseguenza di dover provvedere manualmente alla loro ricostruzione;
   - un servizio subisce un'interruzione significativa ("black out" elettrico o attacchi di tipo "denial of service").

Qualora il numero degli interessati dalla violazione, o potenziali interessati, sia ridotto e questi siano identificabili, è opportuno prestabilire degli elenchi da utilizzare nel caso in cui il titolare ritenga necessario inviare loro delle comunicazioni personalizzate.

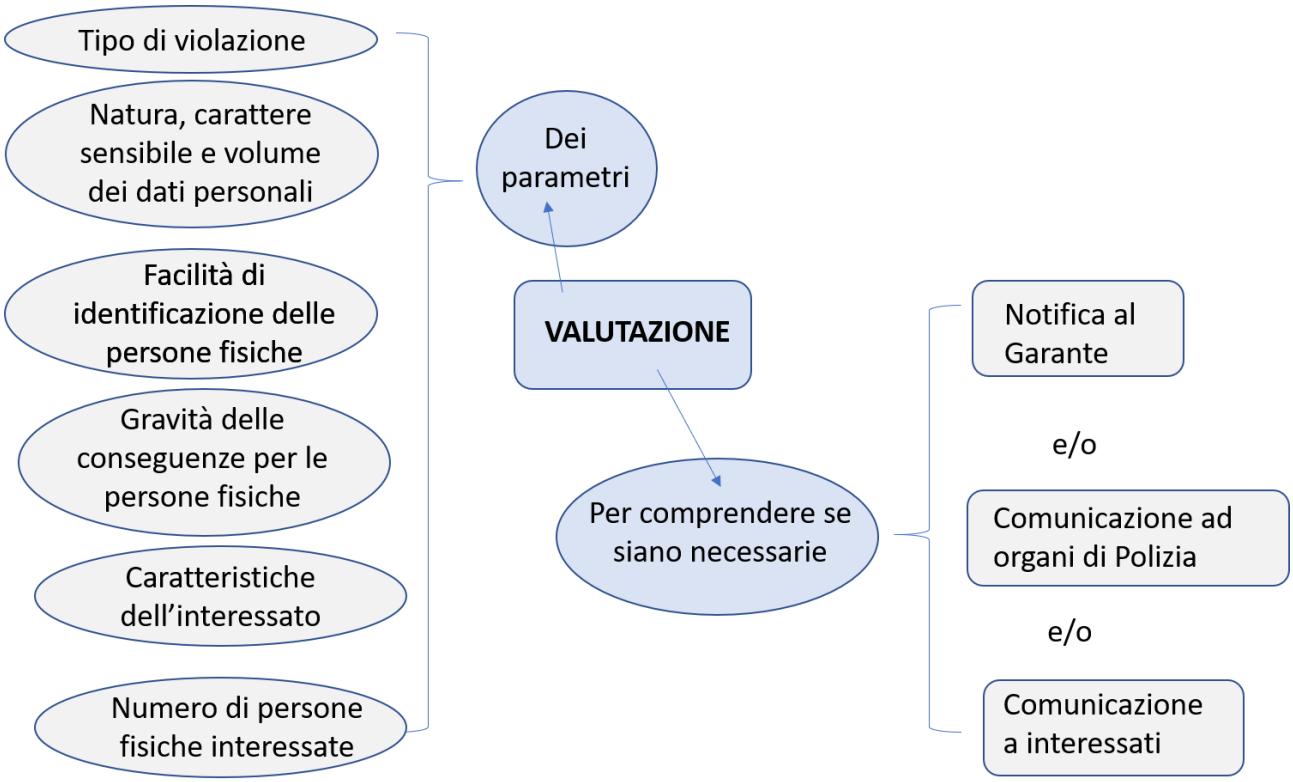
C. ANALISI APPROFONDITA E/O SUPPLEMENTARE

L'analisi supplementare viene attivata **solo se sono necessarie informazioni aggiuntive** rispetto a quella già eseguita. Ad esempio:

- il titolare ritiene di dover operare un approfondimento finalizzato all'integrazione di una notifica al Garante;
- l'Autorità Garante, gli organi di polizia o la magistratura ritengono necessarie informazioni aggiuntive o approfondimenti di informazioni già fornite;
- durante una delle fasi del processo digestione del *Data Breach* sono emerse situazioni che non potevano precedentemente essere approfondite;
- non è stato possibile coinvolgere pienamente i responsabili del trattamento ex art. 28 GDPR o questi non hanno comunicato in tempo utile i risultati delle loro analisi.

L'analisi supplementare può essere attivata più volte per la stessa violazione.

FASE N. 3 – VALUTAZIONE (2° momento))



La responsabilità di questa fase è in capo al titolare, che può avvalersi eventualmente dei responsabili del trattamento ex art. 28 GDPR.

Il titolare deve **valutare il rischio** che effettivamente deriverebbe da una violazione avvenuta, **al fine di decidere se**:

- **notificare la violazione al Garante**, stabilendo in che modo eseguirla (ad es. in più fasi); la notifica va inoltrata se il titolare ritiene **probabile** che la violazione comporti **rischi per i diritti e le libertà delle persone**;
- **comunicare la violazione agli interessati**, stabilendo in che modo (art. 34 GDPR); la comunicazione va eseguita se il titolare ritiene che gli interessati possano subite un **rischio elevato per i loro diritti e libertà**;
- **comunicare la violazione agli organi di polizia**, quando è accertato che violazione deriva da un **comportamento illecito o fraudolento**;
- richiedere ulteriori verifiche tecniche necessarie per un'ulteriore comunicazione.

L'esecuzione delle attività di notifica o comunicazione è successivamente descritta.

Per compiere tale valutazione, il titolare deve tenere preliminarmente in conto le **circostanze della violazione**[1].

Le Linee Guida del WP 29 enumerano, illustrano ed esemplificano alcuni **parametri circostanziali utili alla valutazione del rischio** per le libertà e i diritti delle persone fisiche:

- **Tipo di violazione**

Il tipo di violazione verificatasi può influire sul livello di rischio. Ad esempio, in caso di violazione di dati sanitari, la perdita della loro riservatezza può comportare conseguenze dannose qualitativamente e quantitativamente differenti, rispetto alla perdita della loro integrità e disponibilità.

- **Natura, carattere sensibile e volume dei dati personali**

Elemento fondamentale della valutazione del rischio è la tipologia dei dati personali che sono stati compromessi dalla violazione. Solitamente **più i dati sono sensibili, maggiore è il rischio** di danni per le persone interessate.

Tuttavia, non è soltanto la sensibilità dei dati in sé e per sé considerati ad essere un fattore influente, ma **anche il contesto in cui i dati personali sono raccolti**, il quale potrebbe richiedere maggiore attenzione nel loro trattamento.

Ad esempio, è improbabile che la divulgazione del nome e dell'indirizzo di una persona fisica in circostanze ordinarie causi un danno sostanziale; tuttavia, se i medesimi dati appartengono a un genitore adottivo e vengono comunicati al genitore biologico, le conseguenze potrebbero essere molto gravi, tanto per il genitore adottivo quanto per il bambino.

Inoltre, **la violazione di più dati personali combinati fra loro ha conseguenze più dannose**, rispetto a quella di un singolo dato. 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 addirittura ottenere un'usurpazione d'identità.

- **Facilità di identificazione delle persone fisiche**

Un fattore importante da considerare è la facilità con cui soggetti non autorizzati possano identificare persone fisiche, o semplicemente venendo a conoscenza dei loro dati (senza la necessità di ulteriori ricerche), oppure abbinandoli con altre informazioni che le riguardino. La riuscita dell'identificazione dipende non solo dai dati oggetto di violazione, ma anche dal contesto specifico in cui avviene la violazione, nonché dalla disponibilità pubblica dei corrispondenti dettagli personali.[2]

- **Affidabilità dei destinatari delle comunicazioni di dati errati**

[1] A questo proposito, il considerando n. 88 del GDPR puntualizza che: "*Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, **è opportuno tenere debitamente conto delle circostanze di tale violazione**, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali*".

[2] A questo proposito una buona regola di sicurezza è la pseudonimizzazione dei dati. 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 (definita all'articolo 4, n. 5 GDPR, come *"il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile"*) 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.

Occorre **anche valutare la pericolosità del soggetto non autorizzato alla conoscenza dei dati**, la cui violazione potrebbe essere di per sé inoffensiva. Si pensi ad esempio al caso di un ladro professionista che venga a conoscenza dell'elenco dei clienti abituali di forniture, i quali abbiano, durante il periodo di loro assenza per ferie, chiesto momentaneamente l'interruzione del servizio.

La circostanza che il titolare del trattamento sappia o meno se i dati personali siano stati trasmessi a destinatari affidabili o inaffidabili può incidere sulla valutazione del livello di rischio potenziale: infatti, **l'affidabilità del destinatario può neutralizzare la gravità delle conseguenze della violazione**. Il che non significa che quest'ultima non si sia realizzata, ma che la probabilità del rischio per le persone fisiche verrebbe annullata, venendo meno, quindi, la necessità della notifica all'Autorità Garante o alle persone fisiche interessate. Si ipotizzi il caso in cui il titolare invia accidentalmente dei dati personali all'ufficio sbagliato di un'azienda con cui ha costanti rapporti: si verifica una violazione che, in prima battuta, impone al titolare di chiedere al destinatario di restituire o distruggere in maniera sicura i dati ricevuti. Poiché il titolare del trattamento ha una relazione continuativa col destinatario, verosimilmente conosce le sue misure di sicurezza, tanto da ritenerlo "affidabile": può dunque ragionevolmente aspettarsi che non utilizzerà illecitamente le informazioni conosciute per errore.

- **Caratteristiche particolari dell'interessato**

Una violazione può riguardare dati personali relativi a minori o ad altre persone fisiche vulnerabili, soggette a un rischio più elevato di danno. Altri fattori concernenti la persona fisica potrebbero influire sul livello di impatto della violazione sulla stessa.

- **Caratteristiche particolari del titolare del trattamento di dati**

La natura e il ruolo del titolare del trattamento e delle sue attività possono influire sul livello di rischio per le persone fisiche in seguito a una violazione. Se, ad esempio, un'organizzazione medica tratta categorie particolari di dati personali, mentre un quotidiano soltanto dati personali comuni, la conseguenza è chela violazione di una mailing list della prima comporterebbe effetti più gravi rispetto a quelli ne deriverebbero dalla violazione della seconda.

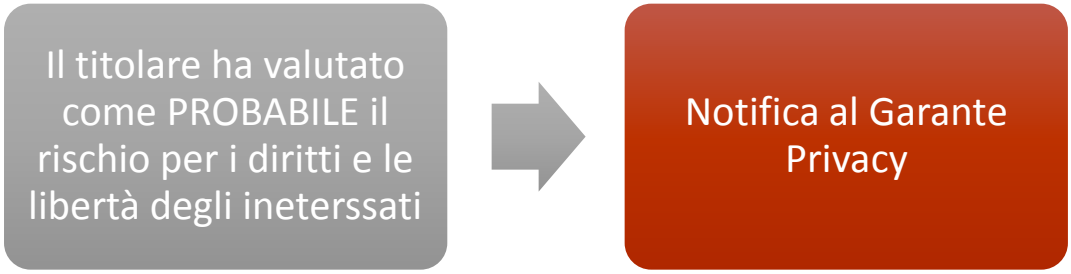
- **Numero di persone fisiche interessate**

Una violazione può riguardare solo una o poche persone fisiche, oppure diverse migliaia. Di norma, maggiore è il numero di persone fisiche interessate, più grave è l'impatto che una violazione può avere.

- **In caso di dubbio?**

Alla luce dei criteri qui sopra illustrati,nelvalutareilrischiochepotrebbederivaredaunaviolazione,iltitolaredeltrattamentodovrebbeconsideraretantolagravitàdell'impattopotenzialesuidirittiesullelibertàdellepersonefisiche,quantolaprobabilitàchetaleimpattosiverifichi.Seleconseguenzediunaviolazione sono più gravi, il rischio è più elevato; analogamente, se la probabilità che tali conseguenze siverifichinoèmaggiore,maggioreèancheilrischio.**Incasodidubbio,iltitolaredeltrattamentopuò prudentemente effettuare la notifica**.

FASE N. 4 – NOTIFICA AL GARANTE (3° momento)



Se il titolare ritiene probabile il rischio per i diritti e le libertà degli interessati, allora deve procedere con la notifica al Garante della Privacy.

Il titolare deve aver presente le seguenti **REGOLE:**

1. La notifica dev'essere eseguita entro il **termine**, non tassativo, di**72 ore dal momento in cui il titolare è venuto a conoscenza della violazione**. Se non si osserva tale prescrizione, il titolare deve corredare la comunicazione con la giustificazione del ritardo (par. 1 Art. 33 GDPR), che, peraltro, potrebbe causare ulteriori controlli da parte del Garante con le conseguenti possibili sanzioni. Tale prescrizione temporale permette al titolare di avere un parere autorevole circa la comunicazione o meno della violazione ai soggetti interessati.
2. Il WP29 chiarisce che **l'obiettivo** dell'obbligo di notifica è quello di **incoraggiare i titolari ad agire prontamente in caso di violazione**, contenendo i possibili danni, recuperando, se possibile, i dati personali compromessi e chiedendo il parere all'autorità di controllo.
3. Il WP29 raccomanda che il titolare informi comunque l'autorità di vigilanza (notifica al Garante) il più presto possibile, **anche se non possiede tutte le informazioni** richieste e non ne conosca quindi la portata, per poi provvedere in un momento successivo all'integrazione della notifica. L'obbligo di notifica è soddisfatto anche se adempiuto in più fasi, come concesso dal Regolamento Europeo (paragrafo n. 4 dell'art. 33): ***"****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"*.
4. Il WP29, nelle sue linee guida, precisa che la mancata comunicazione può essere sanzionata, ma che **nessuna sanzione è prevista nel caso di comunicazione incompleta o di comunicazione non necessaria**.
5. Qualora una violazione dei dati personali coinvolga dati di persone fisiche in più Stati membri, il titolare deve notificare la violazione all'Autorità di controllo capofila.

Il paragrafo n. 3 dell'art. 33 sopracitato definisce il **contenuto minimo della notifica**. Essa 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 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 le misure che il titolare si propone di adottare per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

In data 05.08.2019, il Garante ha pubblicato sul suo sito internet un modello di notifica del *Data Breach*. La pagina web è la seguente:
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9128501.

Il modello è allegato al presente documento (**Allegato 2**).

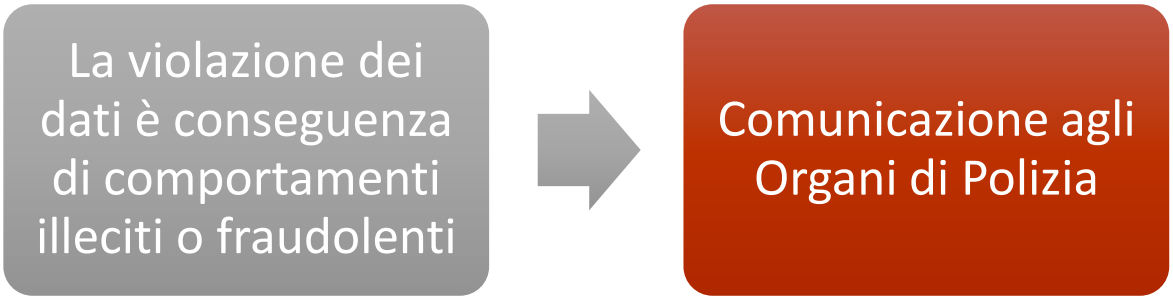
AZIONI OPERATIVE

La notifica deve essere inviata al Garante tramite posta elettronica certificata all'indirizzo **protocollo@pec.gpdp.it** oppure tramite posta elettronica ordinaria all'indirizzo **protocollo@gpdp.it** e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "NOTIFICA VIOLAZIONE DATI PERSONALI" e opzionalmente la denominazione del titolare del trattamento.

FASE N. 5 – SEGNALAZIONI AGLI ORGANI DI POLIZIA (3° momento)

SEGNALAZIONE AGLI ORGANI DI POLIZIA



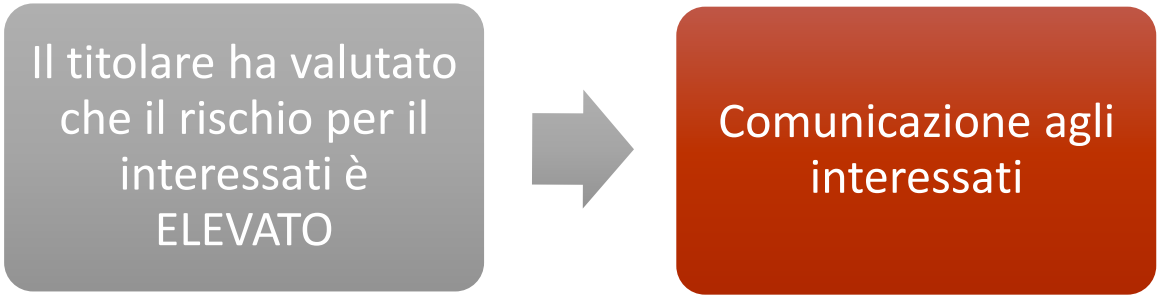
Occorre sempre effettuare **denuncia agli organi di polizia quando la violazione ai dati sia conseguenza di comportamenti illeciti o fraudolenti.**

Oltre alle modalità conosciute per eseguire comunicazione o denuncia agli organi di polizia, per alcune tipologie di *Data Breach*, è possibile eseguireunacomunicazionetelematica:infatti,datempoèstato attivato un sito internet della Polizia Postale e delle Comunicazioni raggiungibile all'indirizzo http://www.commissariatodips.it/.

All'interno di queste pagine si possono reperire utili notizie sui tentativi di reato in corso ed eseguire denunce o segnalazioni di reati telematici, previa registrazione.

Si precisa che l'incidente di sicurezza informatico va segnalato anche al "Computer Security IncidentResponse Team – Italia" (CSIRT), qualora non si tratti di vulnerabilità già note a tale ente e da esso quindi già catalogate (https://csirt.gov.it/segnalazione).

FASE N.6 – COMUNICAZIONE AGLI INTERESSATI (3° momento)



L'obbligo di dare **comunicazione agli interessati** di una violazione dei dati personali che li riguardano è previsto all'art. n. 34 del GDPR, **quando la violazione è suscettibile di prestare rischio ELEVATO per i diritti e le libertà delle persone fisiche** (paragrafo n. 1).

L'art. 34 del GDPR stabilisce che la comunicazione agli interessati dev'essere eseguita ***"senza ingiustificato ritardo"***: ne consegue che ad essa si possa procedere anche prima o contestualmente alla notifica al Garante, senza cioè attendere una sua imposizione (contribuendo peraltro a mitigare eventuali sanzioni);

La comunicazione agli interessati **non è richiesta quando** (par. 3 art. 34 del GDPR:

a) il titolare del trattamento aveva messo in atto le misure di protezione, tecniche e organizzative, adeguate 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) la comunicazione richiederebbe sforzi sproporzionati; in tal caso, il titolare può effettuare una comunicazione pubblica o una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Al paragrafo n. 2 dello stesso art. 34 viene precisato che **la comunicazione deve descrivere**, con un **linguaggio semplice e chiaro**, la natura della violazione dei dati personali e deve contenere almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del GDPR.

Deve cioè contenere le seguenti informazioni:
- il nome e i dati di contatto del responsabile della protezione dei dati o altro punto di contatto;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui il titolare si propone l'adozione per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'Autorità di Controllo può richiedergli di provvedervi se nessuna delle condizioni di cui al paragrafo 3 sia soddisfatta (paragrafo 4 dell'art. 34 del GDPR).

ACCOUNTABILITY E REGISTRAZIONE DELLE VIOLAZIONI

L'art. 33, paragrafo n. 5 del GDPR **prescrive al titolare di documentare qualsiasi violazione dei dati personali**, al fine di consentire all'autorità di controllo di verificare il rispetto della normativa.

Ciò significa che le attività svolte in ciascuna delle fasi devono essere documentate e, quindi, rese tracciabili, replicabili, riportando le violazioni, le circostanze, le conseguenze ed i rimedi.

Inoltre, il WP29 raccomanda di documentare la motivazione delle decisioni assunte a seguito di una violazione; in particolare, se una violazione non è stata notificata, richiede di specificare i motivi per cui il titolare del trattamento abbia ritenuto improbabile che la violazione comportasse un rischio per i diritti e le libertà delle persone fisiche. Allo stesso modo, se il titolare del trattamento ritiene che ricorrano le condizioni per cui *non* è richiesta la comunicazione all'interessato (Art. 34 paragrafo n. 3 del GDPR), deve essere in grado di provare adeguatamente tale sussistenza.

TENUTA DEL REGISTRO DEGLI INCIDENTI DI SICUREZZA E DELLE VIOLAZIONI DEI DATI PERSONALI

L'**Allegato n. 1** del presente documento è costruito in modo tale da documentare l'intera gestione del Data Breach e quindi può essere utilizzato anche per la costruzione del "Registro delle violazioni".

Nel registro, dovrà essere inserita in un'apposita scheda riguardante ogni incidente, anche se l'evento non ha generato violazione dei dati personali.

Per garantire **l'immodificabilità** del registro, è necessario che ad ogni inserimento o variazione venga eseguita un'esportazione in formato PDF del documento, firmato digitalmente dal legale rappresentante dell'ente titolare (o da suo delegato) e denominato utilizzando un numero progressivo per evidenziarne la versione.

III. MATRICE DI ASSEGNAZIONE DELLE RESPONSABILITÀ

In questa sezione del documento, sono poste in relazione le principali risorse umane con le attività delle quali sono responsabili per l'attuazione delle varie fasi del processo di *Data Breach*. La matrice utilizzata per l'accoppiamento è denominata "RACI".

Di seguito sono fornite due diverse matrici:

1) la prima contempla le attività da eseguire in caso di *Data Breach* impattante su risorse informatiche,
2) la seconda per le attività relative ad incidente su risorse analogiche.

Nel caso di *Data Breach* che impatti su risorse sia informatiche sia analogiche, si dovranno seguire entrambe le matrici per la parte di riferimento.

La matrice prende la propria denominazione dalle iniziali dei ruoli previsti (in lingua inglese) per l'esecuzione delle attività dei processi aziendali. I ruoli previsti dalla matrice sono:

FIGURA	DESCRIZIONE DELLA FIGURA
R - (Responsible)	È il responsabile dell'**esecuzione** dell'attività; è, quindi, colui che o la dirige direttamente o ha dato mandato ad altri soggetti di gestirla per suo conto; possono esserci più R per ogni attività;
A - (Accountable)	È il responsabile dell'**attività** e/o colui che la approva (ci può essere una sola A per ogni attività)
C - (Consulted)	È il consulente (possono essere più di uno), che supervisiona e/o dà consulenza all'attività dei responsabili (A ed R)
I – (Informed)	Sono le persone (fisiche o giuridiche, interne od esterne) che non hanno bisogno di essere coinvolte attivamente nella parte del progetto in capo all'ente, ma che devono essere informate circa l'andamento dell'attività.

DEFINIZIONE DELLE FIGURE COINVOLTE

Una persona fisica può ricoprire anche simultaneamente più figure.

FIGURA	DESCRIZIONE DELLA FIGURA
Titolare	Istituto scolastico; le azioni sono compiute dal suo legale rappresentate (Dirigente) o suo sostituto
Responsabile della protezione dei dati (DPO)	Responsabile della Protezione dei Dati (art. 37 GDPR)
Delegato al trattamento	Soggetto delegato dal Titolare a gestire a conformità delle attività di trattamento rispetto alla normativa privacy

Responsabile del trattamento dei dati ex art. 28 GDPR	Persona fisica o giuridica che tratta i dati personali per conto del Titolare (art. 28 GDPR)
Responsabile dei sistemi informativi	Soggetto delegato dal Titolare per sovrintendere alle operazioni di trattamento eseguite con strumenti informatici. La figura può coincidere con quella di responsabile per la transazione al digitale (art. 17 CAD)
Garante Privacy	Autorità nazionale a tutela dei diritti derivanti dalle norme sulla protezione dei dati personali
Forze dell'ordine	Organo di polizia o Magistratura a cui viene denunciata la violazione di sicurezza se ne ricorrono gli estremi
Interessati	Persone fisiche i cui dati sono stati coinvolti nell'incidente

MATRICE RACI PER *Data Breach* IMPATTANTE SU RISORSE INFORMATICHE

FASI	1	2	3	4	5	6	7
Figure coinvolte	Rilevazione Acquisizione	Gestione Tecnica e Analisi	Valutazione	Notifica al Garante	Segnalazioni (Forze dell'ordine e CERT-PA)	Comunicazioni interessati e riscontri	Registrazione della violazione
Titolare	I	I	A	A	A	R	A
DPO	C	C	C	R	C	R	C
Delegato/i al trattamento	R	R	R	R	R	R	R
Resp. trattamento dati ex art. 28 GDPR (se coinvolto)	R	R/A	R	R	R	R	C
Resp. dei sistemi Informativi	R	A/R	C	R	R	R	C
Garante Privacy				I		I	I
Forze dell'ordine					I		
Interessati						I	

MATRICE RACI PER *Data Breach* IMPATTANTE SU RISORSE ANALOGICHE

FASI	1	2	3	4	5	6	7
Figure coinvolte	Rilevazione Acquisizione	Gestione Tecnica e Analisi	Valutazione	Notifica al Garante	Segnalazioni (Forze dell'ordine)	Comunicazioni interessati e riscontri	Registrazione della violazione
Titolare	I	I	A	A	A	R	A
Referente privacy	I	I	C	I	I	I	I
Resp. Anticorruzione e Trasparenza		C	C	I	I	I	I
DPO	C	C	C	R	C	R	C
Delegato/i interno al trattamento	R	R	R	R	R	R	R
Resp. Trattamento Esterno (se coinvolto)	R	R/A	R	R	R	R	C
Resp. comunicazione		I	I	I		A	I
Resp. Archivi	A	A/R	C	R	R	R	I
Resp. Violazione		C	I		I		
Garante Privacy				I		I	I
Forze dell'ordine					I		
Interessati						I	

ALLEGATI

Si devono considerare come parte integrante di questo documento tutti gli allegati approvati con lo stesso, in particolare:

- Allegato n. 1 – Modello di segnalazione e gestione di *Data Breach*
- Allegato n. 2 – Modello di notifica al Garante per la Protezione dei Dati Personali di *Data Breach*.

AGGIORNAMENTO DEL PRESENTE DOCUMENTO E DEGLI ALLEGATI

Sulla base dell'evolversi della normativa e del pensiero in materia di protezione dei dati personali, potrà presentarsi la necessità di aggiornare o integrare il presente documento.

La frequenza di aggiornamento non può essere stabilita a priori.

Qualora le autorità o gli organismi pubblici mettessero a disposizione modelli di comunicazioni o metodologie di comunicazione che sostituiscano i modelli qui riportati, si dovranno immediatamente adottare le disposizionipervenuteedilpresentedocumentoe/oisuoiallegatipotrannoessere modificati anche in tempi successivi.

Allo stesso modo ci si dovrà comportare, se l'applicativo informatico per l'utilizzo del quale sono in corso di acquisizione i diritti fosse configurato in modo da produrre notifiche, segnalazioni, comunicazioni e registri, utilizzando dei modelli diversi da quelli qui riportati.