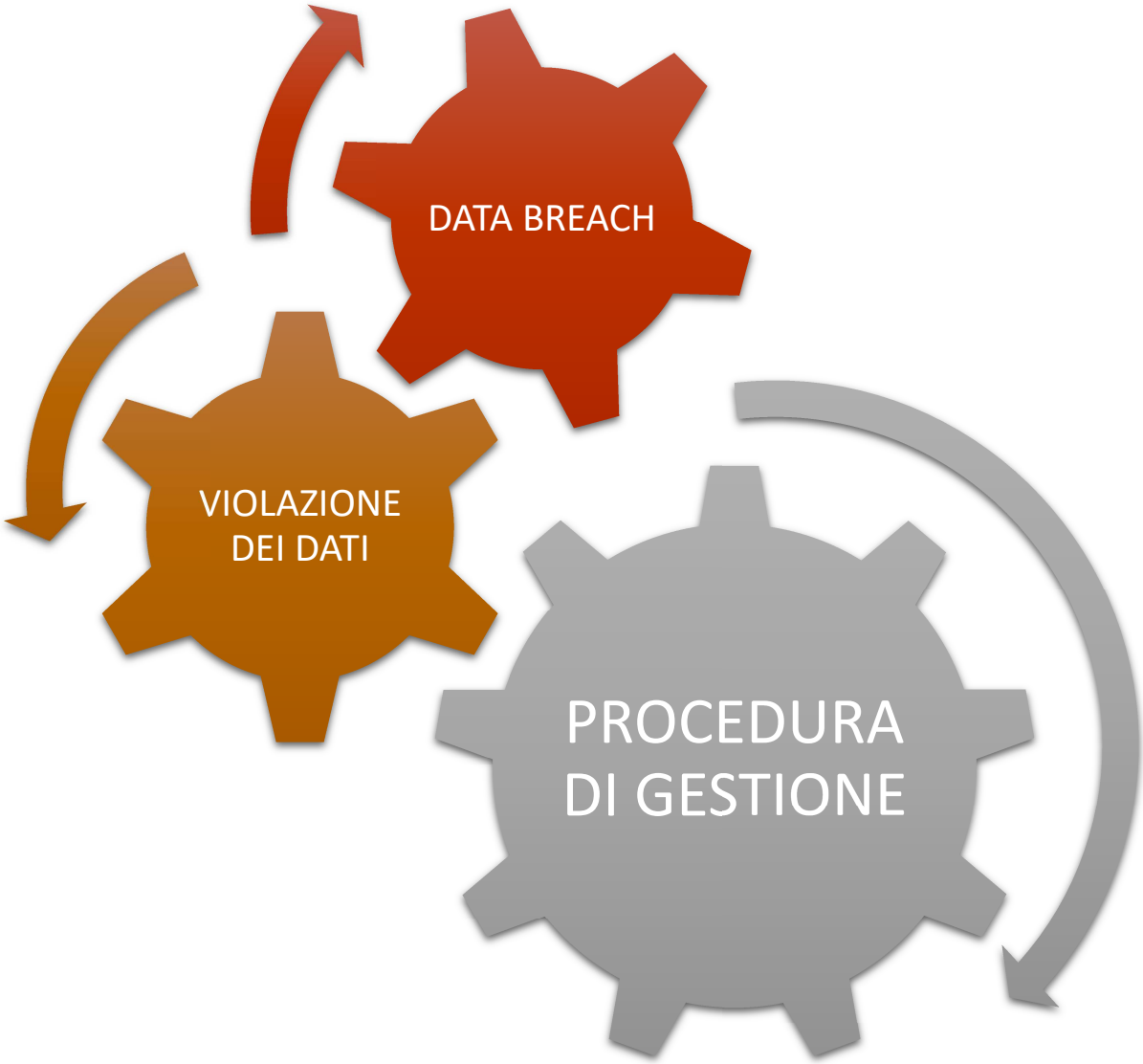


Titolo	Procedura di gestione delle violazioni di dati personali		
Ente	Comune di Cavaglià		
	Allegato B	Versione	00

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 o RGPD	Regolamento (UE) 2016/679 in materia di protezione dei dati personali, nonché della libera circolazione di tali dati. 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.
Codice Privacy	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 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 (Art. 4, par. 1, n. 7 GDPR)
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)
Gruppo di lavoro art. 29	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*)
Accountability	Principio per cui il Titolare deve dimostrare l'adozione di politiche privacy e misure adeguate per dare riscontro, entro i termini stabili dal GDPR, all'esercizio di un diritto dell'interessato in materia di privacy
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
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione

DEFINIZIONE DI DATA BREACH, SCOPO DELLA PROCEDURA E FASI DI GESTIONE

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:

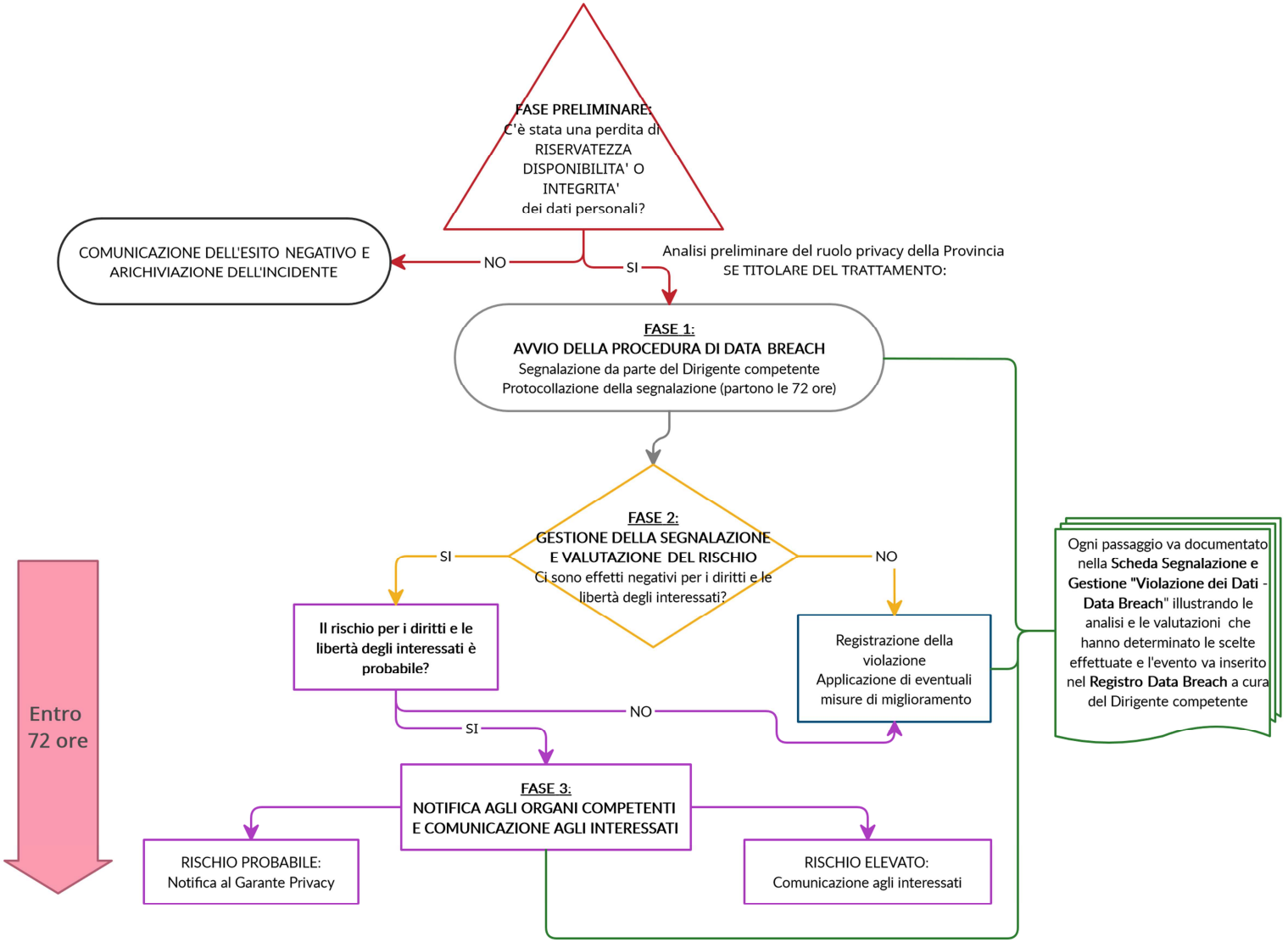
- ✓ la modificazione errata di un database
- ✓ un malware che impedisce l'apertura di una cartella sul server,
- ✓ lo smarrimento di una chiavetta USB, di un telefonino aziendale,
- ✓ l'invio di un dato personale ad un terzo non autorizzato.

Il Regolamento (UE) 2016/679 (c.d. Regolamento Generale sulla Protezione dei Dati personali) ha lo scopo di tutelare i dati personali, e quindi i soggetti interessati, per evitare che un uso non corretto di essi possa danneggiare o ledere le libertà fondamentali e la dignità personale di ognuno.

A tal fine, la presente procedura definisce le attività, i ruoli e le responsabilità che la Casa di Riposo ha previsto per la gestione delle violazioni dei dati personali (Data Breach).

Qui di seguito, vengono schematicamente illustrati i principali passaggi che è doveroso ed opportuno seguire, qualora si verifichi un incidente di sicurezza che possa determinare una violazione di dati personali.

SCHEMA DELLE FASI DI GESTIONE DELLA VIOLAZIONE DEI DATI



MATRICE 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*.

I ruoli previsti dalla matrice sono:

FIGURA	DESCRIZIONE DELLA FIGURA
R - (Responsabile)	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: **proceda alla compilazione dell'Allegato 2.1 - Scheda di Registro delle violazioni dei dati "Data Breach" e dell'Allegato 2.2 – Registro di Data Breach**
C - (Coinvolto)	È il soggetto che deve essere coinvolto (possono essere più di uno), che supervisiona e/o dà consulenza all'attività dei Responsabili (R).
I – (Informato)	Sono le persone (fisiche o giuridiche, interne od esterne) che non hanno bisogno di essere coinvolte attivamente nella parte di analisi in capo all'ente, ma che devono essere informate circa l'andamento dell'attività.

	Soggetti di Riferimento	UFFICIO SEGRETERIA E PROTOCOLLO	DELEGATO AL TRATTAMENTO	DPO	RESPONSABILE DEL PROCEDIMENTO	AMMINISTRATORE DI SISTEMA	TECNICO ASSISTENZA SISTEMISTICA	LEGALE RAPPRESENTANTE	GARANTE PRIVACY	FORZE DI POLIZIA	INTERESSATO
FASE	***ATTIVITÀ***										
1. ACQUISIZIONE	Rilevazione e comunicazione dell'evento al Titolare	R	R	I	I	I					
2. GESTIONE TECNICA	Raccolta informazioni, definizione dei soggetti coinvolti, accertamento dell'effettiva sussistenza del Data Breach, analisi del tipo di violazione		C	C	R	C	C				
3. VALUTAZIONE	Occorre valutare se l'incidente abbia provocato una violazione dei dati da cui siano derivati rischi per i diritti delle persone			C	R	C		I			
4. NOTIFICA AL GARANTE	Se dalla violazione dei dati deriva un rischio probabile per i diritti e le libertà degli interessati			C	R	C	C	I	I		
5. SEGNALAZIONE AGLI ORGANI DI POLIZIA	Se la violazione dei dati è effetto di un illecito			C	R	C		I		I	
6. COMUNICAZIONE AGLI INTERESSATI	Se dalla violazione dei dati deriva un rischio elevato per i diritti e le libertà degli interessati			C	R	C		I			I

	ed è necessario raccogliere i riscontri dell'avvenuta comunicazione										

Il responsabile del procedimento è stato individuato nella persona del Sindaco *pro tempore*.

Il DPO, incarico ricoperto da Labor Service Srl, nella persona della Dott.ssa Angela Emanuele è reperibile alla e-mail: ufficio.privacy@labor-service.it ; telefono: 0321 1814220

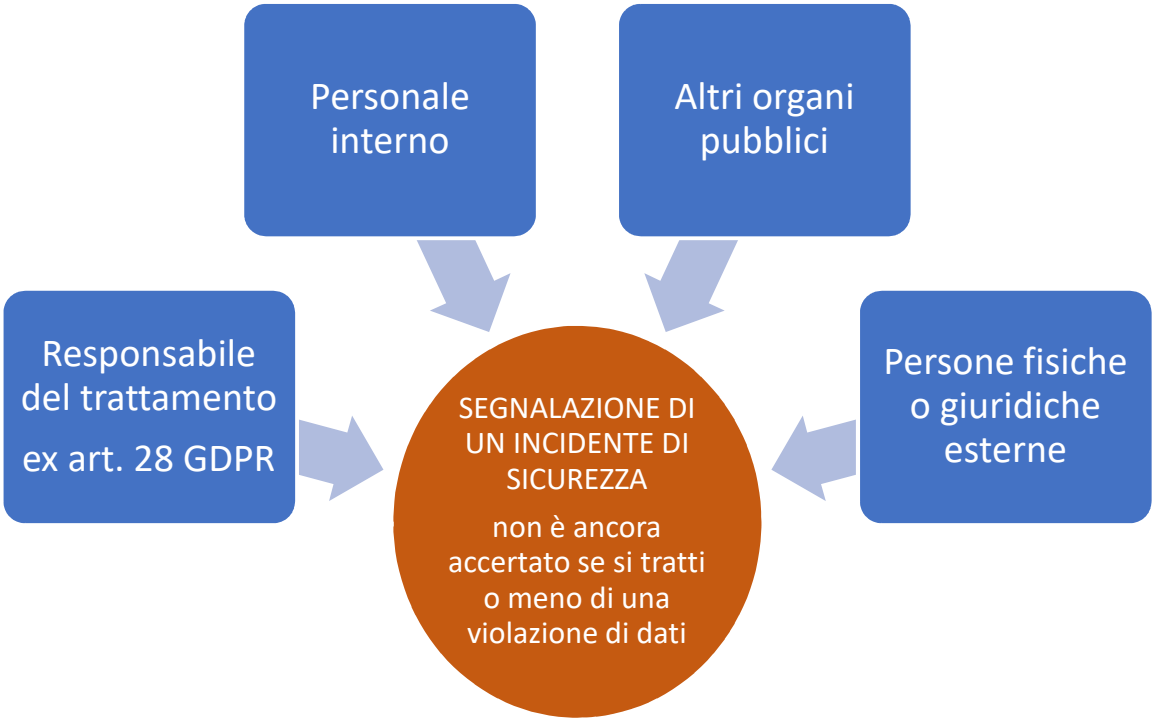
Il servizio di assistenza sistemistica è svolto dalla ditta Nukem Di Giovanni Germinara.

Non sempre i soggetti indicati sopra sono tutti presenti contemporaneamente in ciascuna fase della procedura ma la presenza dipenderà dalla tipologia di violazione e dalle valutazioni che verranno effettuate.

II. MODALITÀ OPERATIVE

FASE 1 – ACQUISIZIONE DELLA SEGNALAZIONE

La rilevazione di un incidente di sicurezza dei dati e la conseguente segnalazione può essere inoltrata da chiunque:



La **Scheda di Segnalazione "Violazione dei dati – Data Breach"** (Allegato 1) è messa a disposizione presso l'ufficio Segreteria - Affari Generali, nonché anche attraverso il sito internet istituzionale. L'ufficio Segreteria - Affari Generali fornirà il supporto necessario alla compilazione della Scheda di Segnalazione, relativamente alla parte indicata come **FASE 1**, che gestirà direttamente l'evento oppure nominerà un Responsabile del procedimento (delegato). La Scheda raccoglie sommariamente le prime informazioni dell'evento che potrebbe incidere sui dati personali e i dati del segnalante in quanto può essere utile in fase di analisi il suo coinvolgimento.

Una volta compilata la Scheda di Segnalazione, la stessa può essere inviata con oggetto "**SEGNALAZIONE VIOLAZIONE DATI**" alla email: cavaglia@ptb.provincia.biella.it; o alla PEC: cavaglia@pec.ptbiellese.it; oppure con consegna a mano presso l'ufficio segreteria, presso la sede degli uffici comunali, in Via Mainelli 8, 13881 Cavaglià (BI)

Preliminarmente, verranno analizzati gli **obblighi dell'Ente in relazione al ruolo che riveste**.

Pertanto, L'Ente:

a) Dovrà gestire direttamente tutte le violazioni dei dati in relazione ai quali **assume la qualifica di Titolare del trattamento** (anche se subite e segnalate da soggetti terzi, ad es. consulente del lavoro che, in qualità di Responsabili del trattamento ex art. 28 GDPR, ha accesso ai dati dei dipendenti);
b) In relazione a particolari trattamenti per i quali dovesse operare **in qualità di Contitolare**, dovrà verificare, nell'accordo stipulato con la/le controparti ai sensi dell'art. 26 GDPR, a chi competa gestire la procedura; se la competenza è dell'altro Contitolare, l'Ente provvederà ad inoltrargli la segnalazione, assicurando comunque quanto riportato al paragrafo seguente e si terrà traccia dell'esito dell'evento; diversamente, se la competenza è propria, gestirà la richiesta come riportato nel punto precedente.
c) In relazione ai trattamenti per i quali **l'Ente operi in qualità di Responsabile del trattamento** ai sensi dell'art. 28 GDPR, avrà l'onere di avvisare, nel più breve tempo possibile, il Titolare del trattamento della violazione dei dati subita e "assistere" il Titolare del trattamento ("Ente Committente") nell'analisi della violazione anche con misure tecniche e organizzative adeguate, là dove possibile, al fine di collaborare nell'adempimento degli obblighi in capo al Titolare in materia di gestione della violazione dei dati conformandosi alle procedure che verranno proposte.

FASE 2 – GESTIONE DELLA SEGNALAZIONE E VALUTAZIONE

Chiarito il ruolo dell'Ente come Titolare del trattamento, prende avvio la fase di **gestione della segnalazione, durante la quale si analizza se ci sia stata una effettiva violazione dei dati** e, di conseguenza, si valuta il rischio per i diritti e le libertà delle persone fisiche derivanti dall'evento. Tali attività sono gestite dal Responsabile del Procedimento, con il coinvolgimento di tutte le figure necessarie per l'analisi dell'evento.

Pertanto, potranno essere **attivati e coinvolti**:

- Personale interno
- Amministratore di Sistema
- Responsabile del trattamento eventualmente coinvolto nella violazione
- Altri soggetti

Questa fase sarà documentata attraverso la compilazione della **Scheda di Segnalazione "Violazione dei dati – Data Breach"** nella parte indicata come **FASE 2** a cura del Responsabile del Procedimento. In tale scheda, si riporterà sommariamente l'indicazione dei soggetti coinvolti, la descrizione dell'evento, le analisi svolte ed il risultato di queste, al fine di determinare se ci sia stata effettivamente una violazione dei dati e procedere così con la valutazione del rischio per i diritti e le libertà delle persone fisiche (saranno allegate alla Scheda di Segnalazione "Violazione dei dati – Data Breach" eventuali relazioni tecniche di analisi e approfondimento).

Le Linee Guida del "Gruppo di lavoro Art. 29"[1] 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 particolare e volume dei dati personali:** 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.
- **Gravità delle conseguenze per le persone fisiche**: a seconda della natura dei dati personali coinvolti in una violazione, ad esempio categorie particolari di dati, il danno potenziale alle persone che potrebbe

[1] Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679 - Adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017 ed emendata e adottata il 6 febbraio 2018

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. 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 che la violazione di una mailing list della prima comporterebbe effetti più gravi rispetto a quelli che 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, nel valutare il rischio che potrebbe derivare da una violazione, l'Ente pubblico dovrebbe considerare tanto la gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche, quanto la probabilità che tale impatto si verifichi. 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. **In caso di dubbio, l'Ente può prudentemente effettuare la notifica**.

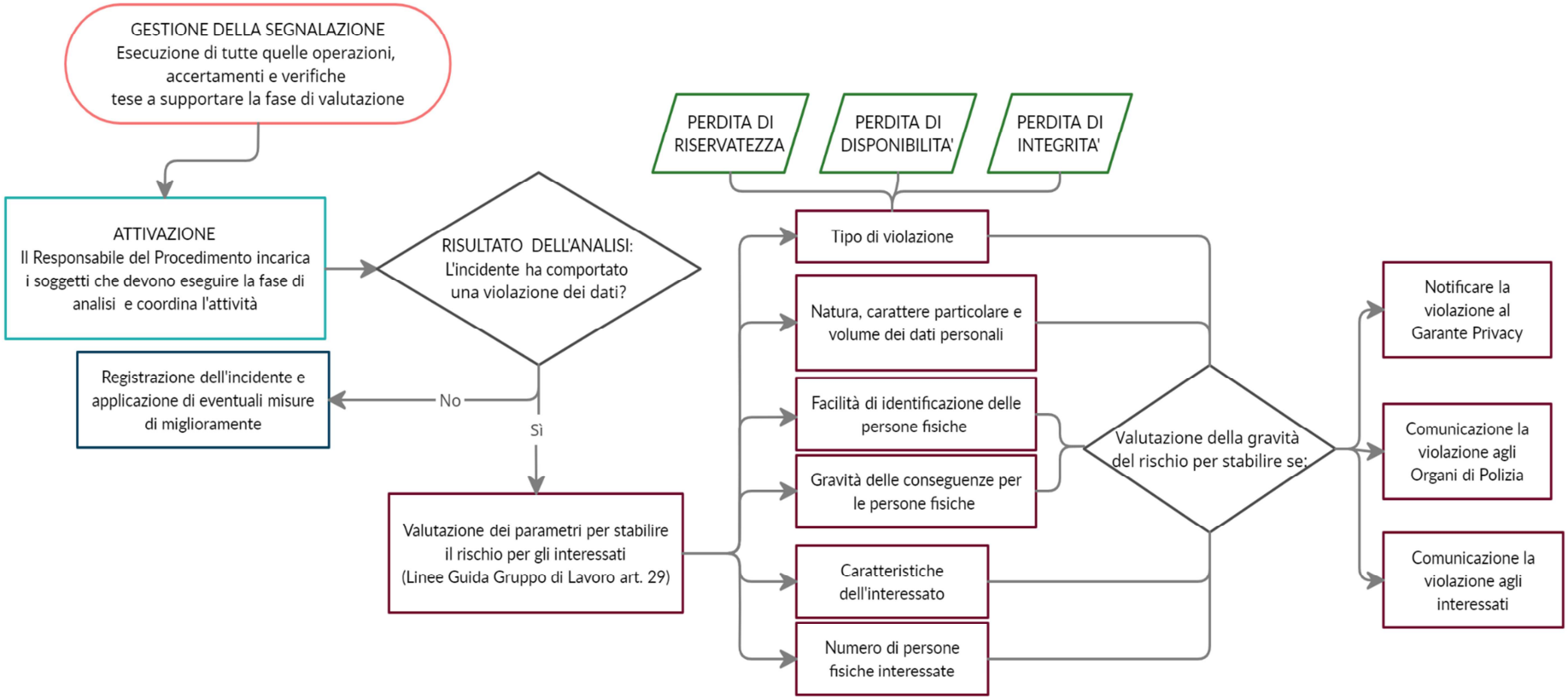
Dal momento in cui il Titolare, in seguito all'analisi dell'incidente, viene a conoscenza che dallo stesso è derivata una violazione dei dati personali (perdita delle loro riservate e/o integrità e/o disponibilità), deve senza ingiustificato ritardo e, ove possibile, entro 72, comunicare la violazione al Garante per la Protezione dei Dati Personali. Qualora la notifica all'Autorità di controllo non sia effettuata entro le 72 ore, va corredata dei motivi del ritardo.

In base al rischio derivante dalla violazione dei dati il Responsabile del Procedimento, insieme al DPO, valuta se:

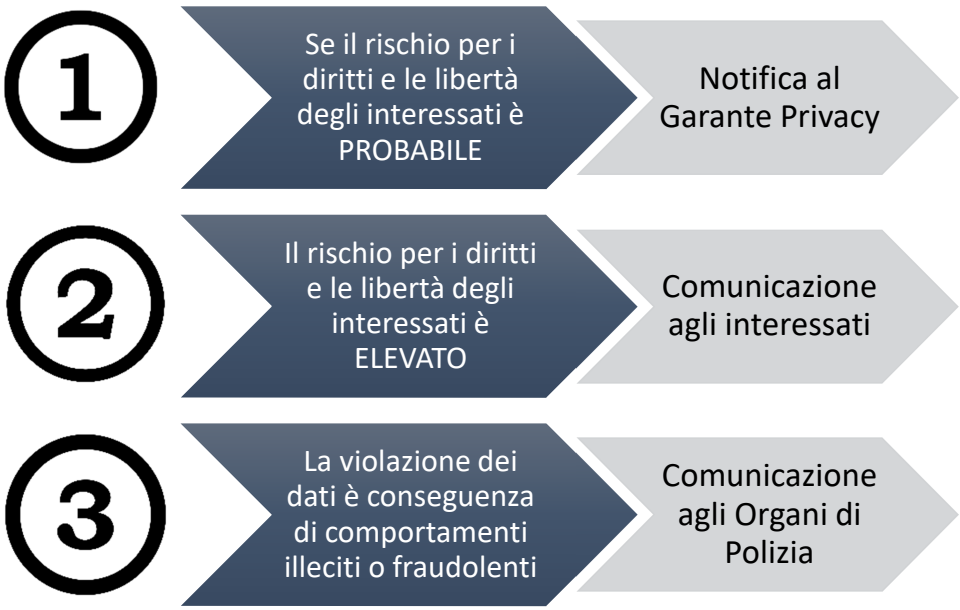
- Notificare la violazione al Garante per la Protezione dei Dati Personali, stabilendo in che modo eseguirla (ad es. in più fasi);
- Comunicare la violazione agli interessati (art. 34 GDPR) stabilendo la modalità;
- Comunicare la violazione agli organi di polizia, quando è accertato che la violazione deriva da un comportamento illecito o fraudolento;

In ogni caso, è necessario **inserire la segnalazione all'interno del Registro Data Breach** (Allegati 2.1 e 2.2.) conservato dall'Ente.

SCHEMA DELLA FASE 2 RELATIVA ALLA GESTIONE DELLA VIOLAZIONE DEI DATI



FASE 3 – NOTIFICA E COMUNICAZIONE AGLI INTERESSATI E ORGANI COMPETENTI



① La **Notifica al Garante per la Protezione dei Dati Personali** dovrà avvenire **senza ingiustificato ritardo e, ove possibile, entro 72 ore** dal momento in cui il Titolare ha valutato che dall'incidente di sicurezza è derivata una violazione dei dati personali. Le notifiche al Garante inoltrate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.

Per effettuare la notifica, occorre seguire le indicazioni riportate sul sito internet istituzionale dell'Autorità: https://www.garanteprivacy.it/regolamentoue/databreach, cliccando su "ACCEDI AL SERVIZIO TELEMATICO DEDICATO AL DATA BREACH" => COMPILAZIONE DELLA NOTIFICA.

Sempre tramite il link indicato, il Garante mette a disposizione anche la possibilità per gli utenti interessati di svolgere una **autovalutazione** per individuare le azioni da intraprendere a seguito di una violazione dei dati personali.

② La **Comunicazione agli interessati** dev'essere eseguita "senza ingiustificato ritardo" e **deve descrivere**, con un **linguaggio semplice e chiaro**, la natura della violazione dei dati personali e deve contenere almeno le seguenti informazioni:

- il nome e i dati di contatto del DPO e del Responsabile del Procedimento o altro punto di contatto;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui la Casa di Riposo si propone l'adozione per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi (azioni correttive che si è deciso di adottare).

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;
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.

③ Per **la Comunicazione o denuncia agli Organi di Polizia** è necessario coinvolgere il Legale Rappresentante che materialmente procederà con tale adempimento anche attraverso delegati.
Per alcune tipologie di illeciti, è possibile eseguire una segnalazione o denuncia (es. denuncia per reati telematici) tramite il sito della *Polizia Postale e delle Comunicazioni* raggiungibile all'indirizzo http://www.commissariatodips.it/.

Allegato 1 - Scheda Segnalazione "Violazione dei Dati – Data Breach"

Il Regolamento (UE) 2016/679 (cosiddetto GDPR) relativo alla Protezione dei Dati Personali prevede la gestione dei DATA BREACH (ovvero "VIOLAZIONI DI DATI") attraverso apposite procedure e moduli di segnalazione. Per violazione di dati personali si intende "La 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". A tale scopo, l'Ente mette a disposizione la presente Scheda per segnalare gli eventi che possono rappresentare una "violazione di dati", secondo la "Procedura Gestione delle violazioni dei dati - Data Breach".

FASE 1 - ACQUISIZIONE DELLA SEGNALAZIONE Compilazione a cura del Segnalante		
INDICAZIONI OPERATIVE PER L'INVIO DELLA SEGNALAZIONE	Il Segnalante al termine della compilazione della FASE 1 della presente Scheda: invia il modulo alla e-mail: cavaglia@ptb.provincia.biella.it Pec: cavaglia@pec.ptbiellese.it oppure consegna il modulo a mano presso l'ufficio segreteria, in Via Mainelli 8, 13881 Cavaglià (BI)	
RESPONSABILE SERVIZIO/AREA	Cognome/Nome	……
DATI RELATIVI AL **SEGNALANTE**	Cognome/Nome	……
	Num. di telefono Indirizzo e-mail	……
	Qualifica	❑ Dipendenti/Collab. ❑ Interessato ❑ Altro ……..

DESCRIZIONE DELL'EVENTO

Circostanze in cui ci si è accorti dell'evento

Data ……/……/…… orario …… circostanza ……

Descrizione dettagliata dell'evento

Descrizione generale della violazione, specificando:

- se c'è stata violazione della riservatezza e/o perdita/distruzione di dati e/o modifica di dati;
- dove è avvenuta la violazione o cosa ha coinvolto (es. indicazione del locale oppure dello strumento)
- tipologia di dati: es. dati anagrafici; dati di contatto (email/numeri di telefono); dati sanitari; dati religiosi; ecc.;
- persone a cui si riferiscono i dati violati (es. utenti del servizio; familiari; operatori; soggetti terzi)
- numero di persone coinvolte dalla violazione (i dati erano relativi ad una sola persona oppure a più persone oppure il numero è indeterminato o non noto);
- eventuali misure di protezione che erano presenti sui dati violati prima della violazione (es. utilizzo di password di accesso; cifratura; dati sotto chiave; utilizzo di iniziali per i dati identificativi ecc.).

……

……

……

Eventuali interventi immediati adottati: ❑ No ❑ Sì, specificare quali:

……

……

INFORMAZIONI SUL TRATTAMENTO DEI DATI ai sensi dell'art.13 Regolamento (UE) 2016/679

Il TITOLARE del trattamento è il Comune di Cavaglià, Codice fiscale 00326680022, Partita IVA 00326680022, in persona del Sindaco pro tempore, Tel. 0161 96038; Fax. 0161 967724; Email: cavaglia@ptb.provincia.biella.it; Pec: cavaglia@pec.ptbiellese.it. I dati anagrafici e di contatto del SOGGETTO SEGNALANTE saranno trattati per le finalità previste dal GDPR e dal Codice Privacy in particolare per dar corso alla segnalazione ed effettuare tutte le verifiche richieste dall'art. 33 GDPR. La base giuridica del trattamento è costituita dall'adempimento di un obbligo legale a cui è tenuto il Titolare del trattamento (art. 33 GDPR). Il conferimento dei dati è facoltativo posto che il Titolare del trattamento ha l'obbligo di analizzare qualsiasi segnalazione relativa a violazioni di dati personali anche se proveniente da soggetto anonimo. I dati personali trattati dal Titolare sono comunicati a terzi destinatari esclusivamente per esigenze operative e tecniche, strettamente connesse e strumentali alla gestione della segnalazione. Potranno essere comunicati dati anche a Forze di Polizia, qualora sia necessario presentare formale denuncia, e al Garante della Protezione dei Dati Personali qualora sia necessario effettuare notifica ai sensi dell'art. 33 GDPR. I dati personali raccolti sono conservati per il periodo necessario per adempiere alle finalità di cui sopra ed in conformità a disposizioni normative. Gli interessati hanno il diritto di ottenere, nei casi previsti, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. GDPR). Inoltre, l'interessato ha il diritto di proporre reclamo ad un'autorità di controllo (www.garanteprivacy.it)

Data compilazione della FASE 1: ……/……/…… **Eventuale allegato:** ❑ No ❑ Sì (specificare……)

Firma Direttore: …… **Firma Segnalante (Eventuale):** ……

Allegato 2.1 – Scheda di registro delle violazioni

Il Regolamento (UE) 2016/679 (cosiddetto GDPR) relativo alla Protezione dei Dati Personali prevede la gestione dei Data Breach (ovvero violazioni di dati) attraverso apposite procedure, moduli di segnalazione e la tenuta di un registro su cui documentare tutte gli incidenti che abbiano, anche solo potenzialmente, violato i dati personali trattati dal titolare.

A tale scopo, il Titolare mette a disposizione la scheda di Registro dove documentare qualsiasi violazione dei dati personali, ai sensi dell'art. 33, par. 5, Regolamento (UE) 2016/679

DATI DEL COMPILANTE (Nome e cognome):	
CONOSCENZA DELL'INCIDENTE DA PARTE DEL TITOLARE (ACQUISIZIONE – FASE 1)	
Modalità con la quale il titolare del trattamento è venuto a conoscenza della violazione:	
Data e ora in cui il titolare del trattamento è venuto a **conoscenza** dell'incidente:	
Data e ora dell'incidente:	
DESCRIZIONE DELL'INCIDENTE	
Descrizione dell'incidente	
Luogo dell'incidente	
Uffici/settori coinvolti	
Descrizione dei sistemi e/o delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione	
GESTIONE DELLA SEGNALAZIONE (GESTIONE TECNICA – FASE 2)	
1. ATTIVAZIONE	
Il titolare ha dato incarico per l'analisi della segnalazione a: ❑ Società informatica esterna: …… ❑ Dipendente o collaboratore interno: …….. ❑ Responsabile del trattamento (art. 28 GDPR): …… ❑ Altro: ……..	

2. ANALISI

Descrizione delle attività di analisi svolte e indicazione delle misure di sicurezza tecniche e organizzative applicate prima dell'evento segnalato:

Causa dell'incidente:

❑ Azione intenzionale interna
❑ Azione accidentale interna
❑ Azione intenzionale esterna
❑ Azione accidentale esterna
❑ Sconosciuta
❑ Altro (specificare):……

Risultato delle attività di analisi:

❑ è una Data Breach (l'incidente ha provocato una violazione di dati personali)
❑ non è una Data Breach (l'incidente non ha provocato una violazione di dati personali)

Natura della violazione:

❑ Perdita di riservatezza (Diffusione/ accesso non autorizzato o accidentale)
❑ Perdita di integrità (Modifica non autorizzata o accidentale)
❑ Perdita di disponibilità (Impossibilità di accesso, perdita, distruzione non autorizzata o accidentale)

Categorie di dati personali oggetto di violazione:

❑ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, indirizzo)
❑ Dati di contatto (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 di navigazione internet, altro)
❑ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
❑ Dati di profilazione
❑ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, altro)
❑ Dati di localizzazione
❑ Dati che rivelino l'origine razziale o etnica
❑ Dati che rivelino opinioni politiche
❑ Dati che rivelino 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
❑ Categorie ancora non determinate
❑ Altro:……

Indicare il volume (anche approssimativo) dei dati personali oggetto di violazione:

❑ N.: ……
❑ Circa n.: ……
❑ Un numero (ancora) non definito di dati:

Categorie di interessati coinvolti nella violazione:
❑ Dipendenti/Consulenti
❑ Cittadini
❑ Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
❑ Associati, soci, aderenti, simpatizzanti, sostenitori
❑ Soggetti che ricoprono cariche sociali
❑ Beneficiari o assistiti
❑ Minori
❑ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
❑ Categorie ancora non determinate
❑ Altro (specificare)

Numero (anche approssimativo) di interessati coinvolti nella violazione:
❑ N. interessati: ……
❑ Circa n. interessati: ……
❑ Un numero (ancora) sconosciuto di interessati

VALUTAZIONE – FASE 3

❑ **Non ci sono potenziali effetti negativi per gli interessati**
❑ **Potenziali effetti negativi per gli interessati:**
- ❑ 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 (specificare)

Stima della gravità della violazione:
❑ Trascurabile
❑ Basso
❑ Medio
❑ Alto
Eventualmente specificare:

Misure adottate a seguito della violazione per ridurre gli eventuali effetti negativi per gli interessati e/o per prevenire simili violazioni future:

COMUNICAZIONE – FASE 4/5/6

Alla luce delle analisi e delle valutazioni svolte si decide di:

❑ Notificare la violazione al Garante Privacy*	❑ NON Notificare la violazione al Garante Privacy
❑ Dare comunicazione agli Organi di Polizia	❑ NON dare comunicazione agli Organi di Polizia
❑ Dare comunicazione ai soggetti interessati	❑ NON dare comunicazione ai soggetti interessati
**V. Allegato 2: Modello di notifica indicato nella Procedura di gestione dei Data Breach*	
Motivare le decisioni in merito alle comunicazioni (allegare le comunicazioni effettuate)	
Eventuali allegati	
Data di termine compilazione:	
Firma:	

Allegato 2.2 – Registro *data breach*

REGISTRO DATA BREACH

ANNUALE:					Totale Data Breach 0			Totale Notifiche al GARANTE PRIVACY 0			Totale Comunicazioni agli interessati 0			
Ricezione della segnalazione (Data + orario)	Comunicazione al DPO	Ruolo Della Casa di Ripso (Titolare/Contitolare/Resp	Soggetti coinvolti (ATTIVAZIONE)	Breve descrizione dell'evento	E' data breach? (si o no)	Natura della violazione	Causa della violazione	Potenziali effetti negativi per i diritti o le libertà degli interessati	Stima della gravità (Trascurabile/Basso/Medio/Alto)	Azioni correttive	Notifica al Garante Privacy (si o no)	Comunicazione agli organi di Polizia (si o no)	Comunicazione agli interessati (si o no)	Note