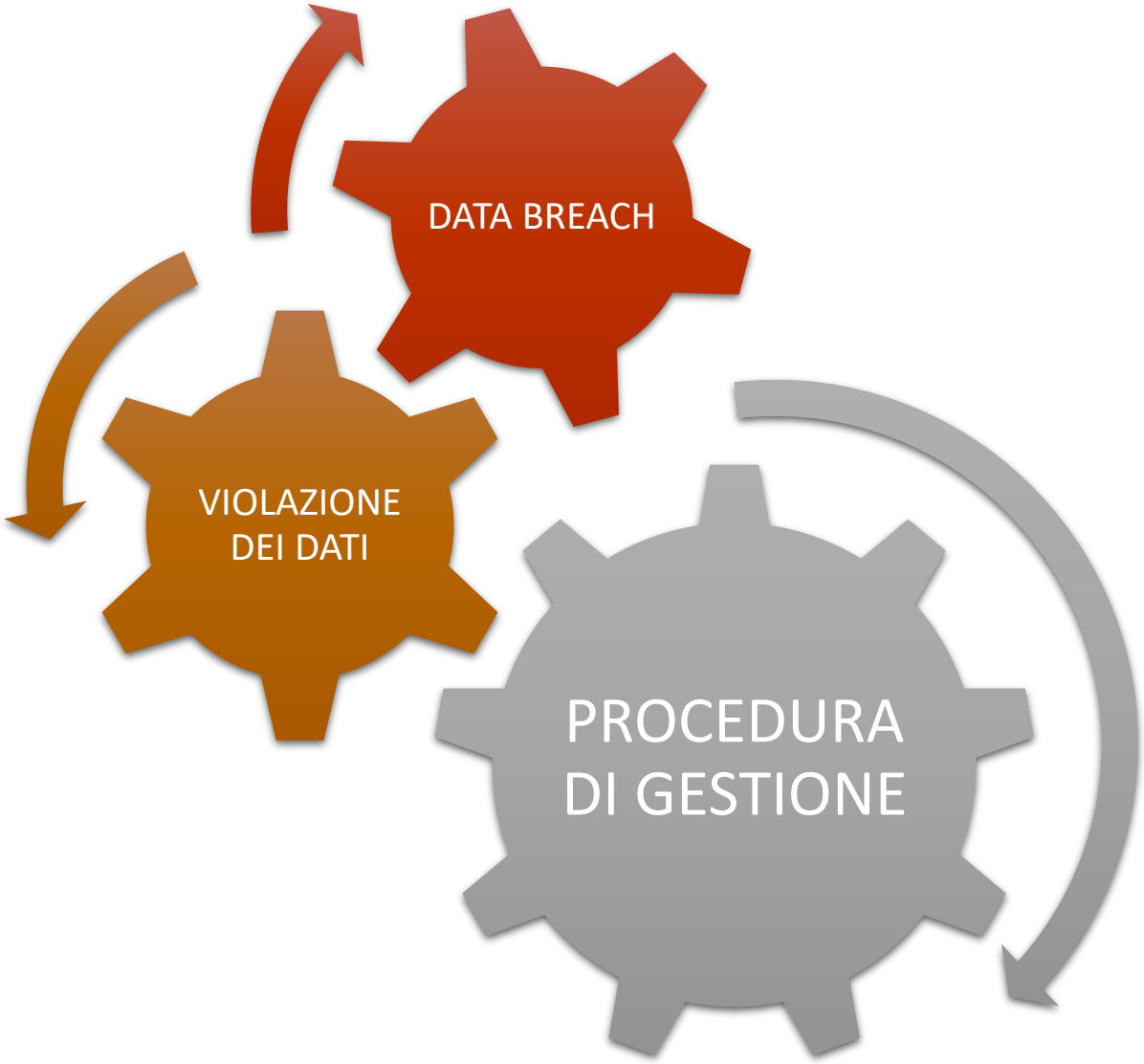


Titolo	Procedura di gestione delle violazioni di dati personali – Data Breach		
Ente	Quattrozeta S.r.l.		
Data di emissione	09/2026	Versione	02

Sommario

I. INTRODUZIONE 3
GLOSSARIO 3
DEFINIZIONE DI DATA BREACH, SCOPO DELLA PROCEDURA E FASI DI GESTIONE 4
MATRICE DI ASSEGNAZIONE DELLE RESPONSABILITÀ 6
MATRICE DELLE RESPONSABILITÀ 6
II. MODALITÀ OPERATIVE 7
GESTIONE PRELIMINARE DELL'INCIDENTE DI SICUREZZA 7
FASE A) - COMUNICAZIONE DI UN INCIDENTE DI SICUREZZA 7
FASE B) – PRESA IN CARICO DELLA COMUNICAZIONE 8
FASE C) – ANALISI DELL'INCIDENTE DI SICUREZZA 8
Le due ipotesi che si possono configurare: 8
FASE D) – ANALISI DEL RUOLO PRIVACY DI QUATTROZETA S.R.L. 8
FASE 1 – AVVIO DELLA PROCEDURA DI DATA BREACH 10
FASE 2 – GESTIONE DELLA SEGNALAZIONE E VALUTAZIONE DEL RISCHIO 10
FASE 3 – NOTIFICA AGLI ORGANI COMPETENTI E COMUNICAZIONE AGLI INTERESSATI 14
AGGIORNAMENTO DEL PRESENTE DOCUMENTO E DEGLI ALLEGATI 15
Allegato 1 - Scheda di segnalazione - "PROCEDURA DI VIOLAZIONE DEI DATI - DATA BREACH" 16
Allegato 2 – Scheda di gestione - "PROCEDURA DI VIOLAZIONE DEI DATI - DATA BREACH" 19
Allegato 3 – Registro Incidenti di sicurezza & Violazione dei dati (c.d. Data Breach) 22

I. INTRODUZIONE

GLOSSARIO

Incidente di sicurezza	Un incidente di sicurezza è un evento (o una serie di eventi) di origine dolosa o accidentale, esterno o interno all'organizzazione, che può comportare la compromissione dei dati detenuti da un'organizzazione.
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 a 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 del trattamento.

Sono, **ad esempio**, potenziali cause di una 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.

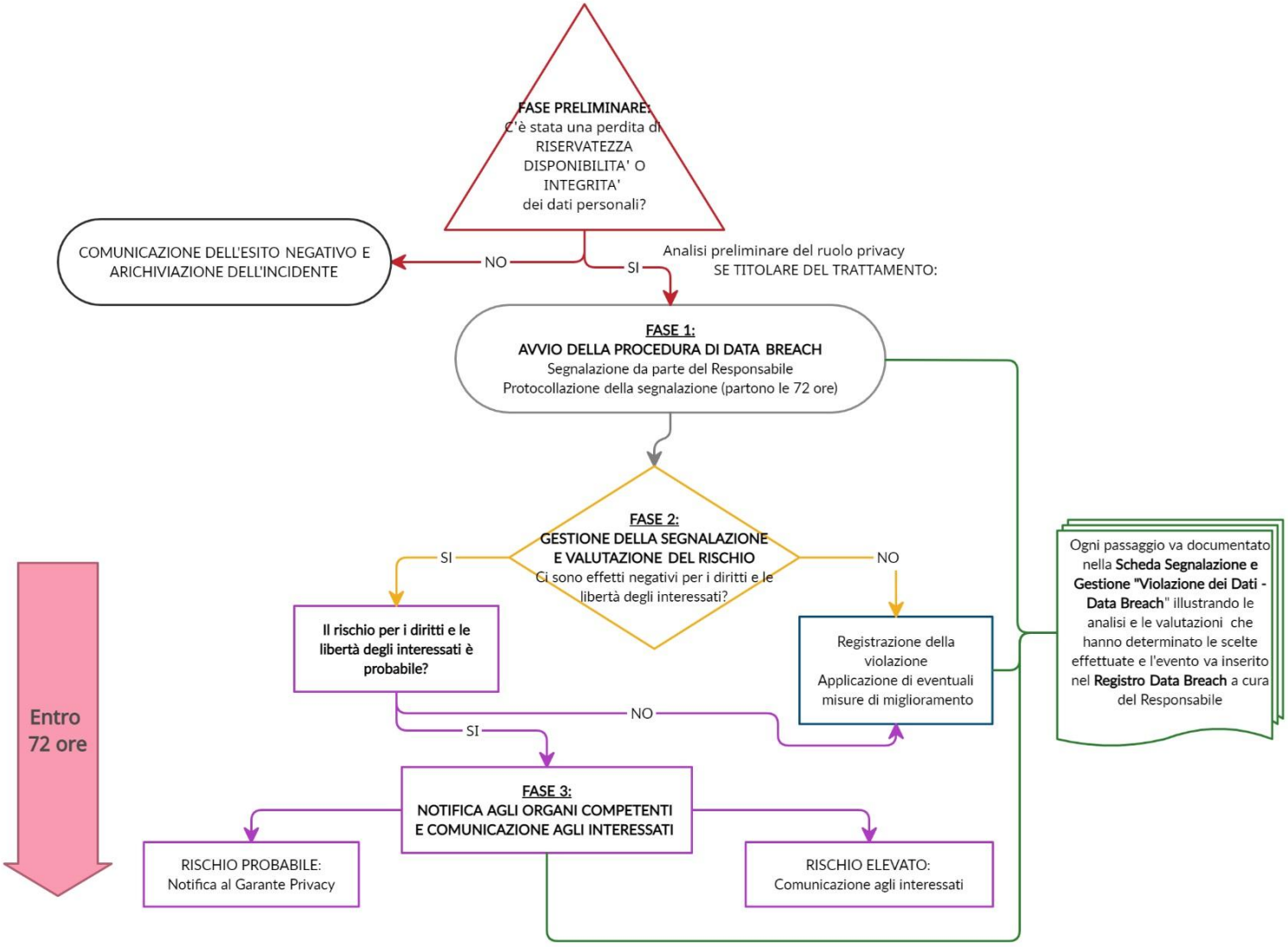
A tal fine, la presente procedura definisce le attività, i ruoli e le responsabilità che la Quattrozeta s.r.l. ha previsto per la gestione delle violazioni dei dati personali (Data Breach).

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.

Da tenere in considerazione **il termine delle 72 ore** per valutare se c'è un rischio per i diritti e le libertà delle persone fisiche conseguenti alla violazione dei dati e se la stessa va notificata al Garante Privacy e comunicata agli interessati.

Il termine decorre da quando il Titolare del trattamento (Quattrozeta) è venuto a conoscenza della violazione dei dati che, in base alla presente procedura, **coincide con la data e l'ora della presa in carico da parte del Responsabile del Procedimento.**

SCHEMA DELLE FASI DI GESTIONE DELLA VIOLAZIONE DEI DATI



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*.

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.
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 alla Società, ma che devono essere informate circa l'andamento dell'attività.

MATRICE DELLE RESPONSABILITÀ

Soggetti di Riferimento		DELEGATO AL TRATTAMENTO	DPO	RESPONSABILE DEL PROCEDIMENTO (Referente privacy interno o suo delegato)	AMMINISTRATORE DI SISTEMA	RESPONSABILE DEL TRATTAMENTO ESTERNO	LEGALE RAPPRESENTANTE	GARANTE PRIVACY	FORZE DI POLIZIA	INTERESSATO
FASE	***ATTIVITÀ***									
1. ACQUISIZIONE	Rilevazione e comunicazione dell'evento al Titolare	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 ed è necessario raccogliere i riscontri dell'avvenuta comunicazione		C	R	C		I			I

II. MODALITÀ OPERATIVE

GESTIONE PRELIMINARE DELL'INCIDENTE DI SICUREZZA

FASE A) - COMUNICAZIONE DI UN INCIDENTE DI SICUREZZA



La gestione dell'incidente di sicurezza si avvia con la comunicazione dell'evento che lo ha generato. La comunicazione dev'essere effettuata, ove possibile, in forma scritta, anche utilizzando mezzi elettronici (es. posta elettronica) e devono essere seguite delle prescrizioni minime:

1. l'**Allegato 1** rappresenta la segnalazione al Titolare di una violazione (reale o presunta), del quale è consigliato l'utilizzo;
2. predisporre la segnalazione in modo tale che sia **più completa e dettagliata possibile**;
3. individuare i precisi **riferimenti temporali** (data ed ora) di quando la segnalazione è stata inoltrata al titolare e da questi acquisita;
4. **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.
5. 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;
6. **il segnalante deve mettersi a completa disposizione del titolare**, per consentirgli di eventualmente integrare le informazioni.

La comunicazione può partire dal personale della Quattrozeta s.r.l., ma non solo; infatti, anche soggetti terzi o utenti dei servizi possono rilevare l'evento venirne a conoscenza. Tali possono procedere direttamente con la segnalazione oppure possono meramente informare Quattrozeta s.r.l., attraverso una email in cui viene descritto l'accaduto. Tale comunicazione dovrà essere inviata al proprio Responsabile avendo cura di verificarne la ricezione o presa di conoscenza.

AZIONI OPERATIVE

1) Il modulo di segnalazione (Allegato 1) viene messo a disposizione sul sito internet istituzionale nella sezione "PRIVACY";

2) Una volta compilato il modulo, è da consegnare a mano presso gli Uffici Amministrativi della Società oppure si può inviare con oggetto "**SEGNALAZIONE VIOLAZIONE DATI**" tramite: E-mail: privacy@quattrozeta.it

FASE B) – PRESA IN CARICO DELLA COMUNICAZIONE

A seguito della ricezione della comunicazione da parte di una persona fisica identificata, il Responsabile prende in carico la comunicazione e verifica se l'evento è di esclusiva competenza della sua Area o se è necessario coinvolgere altre Aree/uffici della società, dandone conto via email al DPO per l'avvio dell'attività di analisi preliminare.

FASE C) – ANALISI DELL'INCIDENTE DI SICUREZZA

Il Responsabile, da solo o insieme agli altri Responsabili eventualmente coinvolti, analizza e valuta se l'incidente di sicurezza ha determinato:

1. **PERDITA DI RISERVATEZZA DEI DATI PERSONALI**
   Esempio: soggetto non autorizzato ha avuto accesso ai dati personali; diffusione di dati personali non autorizzata; furto di documenti o dispositivi informatici che contenevano dati personali ecc.
2. **PERDITA DI INTEGRITÀ DEI DATI PERSONALI**
   Esempio: modifica non autorizzata o accidentale dei dati personali
3. **PERDITA DI DISPONIBILITÀ DEI DATI PERSONALI**
   Esempio: distruzione non autorizzata/accidentale di documenti o strumenti che contenevano dati personali; impossibilità di accesso ai dati personali ecc.

Le due ipotesi che si possono configurare:

A. **Se non si è verificato nessuno di questi casi, il Responsabile comunica tale esito al DPO, così da archiviare l'evento come incidente di sicurezza che è stato analizzato, gestito e concluso.** Tale analisi deve essere indicata all'interno del Registro predisposto (allegato 3). Nello stesso bisognerà specificare che la segnalazione si è conclusa come Incidente di sicurezza, esplicando le motivazioni (es. se era stato segnalato il furto di un faldone, lo stesso è stato ritrovato all'interno degli uffici, magari in un altro armadio; se era stata segnalata la perdita di alcuni dati, gli stessi in realtà erano disponibili in copia backup ecc.);
B. **Se, invece, si è verificato anche uno solo di questi casi, previo eventuale confronto con i soggetti coinvolti, si è di fronte ad una potenziale violazione dei dati personali ed il Responsabile procede con la valutazione del "Ruolo privacy della società" al fine di determinare se la società sia o meno Titolare del trattamento e quindi competente alla gestione della violazione. Se la Quattrozeta s.r.l. è Titolare del trattamento si avvia la gestione della violazione dei dati con la prima fase di segnalazione del Data Breach.**

FASE D) – ANALISI DEL RUOLO PRIVACY DI QUATTROZETA S.R.L.

Il Responsabile, da solo o insieme agli altri Responsabili eventualmente coinvolti, valutato l'incidente di sicurezza come possibile violazione dei dati, analizza il ruolo privacy della Quattrozeta s.r.l.
Infatti, la Quattrozeta s.r.l.:

SE TITOLARE DEL TRATTAMENTO	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. Software House che, in qualità di Responsabili del trattamento ex art. 28 GDPR, ha accesso ai dati della società). La società è Titolare del trattamento dei dati qualora "*determina le finalità e i mezzi del trattamento di dati personali*" (art. 4, par. 1, punto 7) GDPR).

SE CONTITOLARE DEL TRATTAMENTO	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, la Quattrozeta s.r.l. provvederà ad inoltrargli la segnalazione della violazione nelle modalità concordate, assicurando comunque quanto riportato al paragrafo seguente e si terrà traccia dell'esito della segnalazione; diversamente, se la competenza è propria, gestirà la segnalazione di violazione come riportato nel punto precedente. *La società è Contitolare del trattamento dei dati qualora "determina congiuntamente ad altro o altri titolari del trattamento le finalità e i mezzi del trattamento di dati personali"* (art. 26 GDPR).
SE RESPONSABILE DEL TRATTAMENTO	In relazione ai trattamenti per i quali la **Quattrozeta s.r.l. 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 ("Altro Ente/Società") 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. *La società è* Responsabile del trattamento dei dati qualora "*tratta dati personali per conto di altro titolare del trattamento*" (art. 4, par. 1, punto 8) GDPR).



Valutato che la Quattrozeta s.r.l. ha l'onere di gestire la violazione dei dati in quanto Titolare del trattamento o Contitolare del trattamento a cui compete questa attività, il Responsabile procede con l'avvio della procedura di Data Breach attraverso la segnalazione della violazione dei dati.

FASE 1 – AVVIO DELLA PROCEDURA DI DATA BREACH

La **Scheda di Segnalazione e Gestione "Violazione dei dati – Data Breach"** (Allegato 2) è messa a disposizione nella cartella "PRIVACY → Policy e Procedure Privacy → Procedura di gestione delle violazioni dei dati", condivisa fra i diversi uffici di Quattrozeta s.r.l. La compilazione della parte indicata come **FASE 1** è in capo al Responsabile che ha guidato le analisi preliminari e che è tenuto alla segnalazione.

Qualora la violazione sia riferita a più aree organizzative l'avvio (ivi compresa la segnalazione) e la gestione della procedura di Data Breach può essere posta in capo ad un unico soggetto individuato fra i diversi Responsabili.

La Scheda raccoglie sommariamente l'analisi dell'evento che ha determinato la violazione e i dati dei soggetti coinvolti nell'analisi in quanto può essere utile, nelle fasi successive, il loro coinvolgimento.



Al termine della compilazione della Scheda di Segnalazione (FASE 1) si trasmette la stessa, con oggetto "**SEGNALAZIONE VIOLAZIONE DATI,** a:

1. **Email** dedicata alle segnalazioni: privacy@quattrozeta.it
2. Responsabile della Protezione dei dati personali (c.d. **DPO**): privacy@labor-service.it



Da tale momento decorre il termine delle 72 ore per l'analisi del rischio per i diritti e le libertà delle persone fisiche e, nel caso, per la notifica al Garante per la Protezione dei Dati personali.

FASE 2 – GESTIONE DELLA SEGNALAZIONE E VALUTAZIONE DEL RISCHIO

Prende avvio la fase di **gestione della segnalazione in cui si analizza se ci sia un rischio** per i diritti e le libertà delle persone fisiche derivanti dalla violazione dei dati.

Tali attività sono gestite dal Responsabile che ha segnalato la violazione dei dati con il supporto del DPO ed eventualmente di ulteriori soggetti coinvolti (es. Responsabile del trattamento esterno, personale autorizzato al trattamento, Amministratore di Sistema, ecc.).

Il Responsabile avrà cura di compilare la **Scheda di Segnalazione e Gestione "Violazione dei dati – Data Breach"** nella parte indicata come **FASE 2** in cui si riporteranno sommariamente le valutazioni effettuate.

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*

[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

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 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.*

Alla luce dei criteri qui sopra illustrati, nel valutare il rischio che potrebbe derivare da una violazione, la Quattrozeta s.r.l. 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.

Potenziali effetti negativi per gli Interessati (impatto sui diritti e sulle libertà delle persone fisiche):

- Perdita del controllo dei dati personali;

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

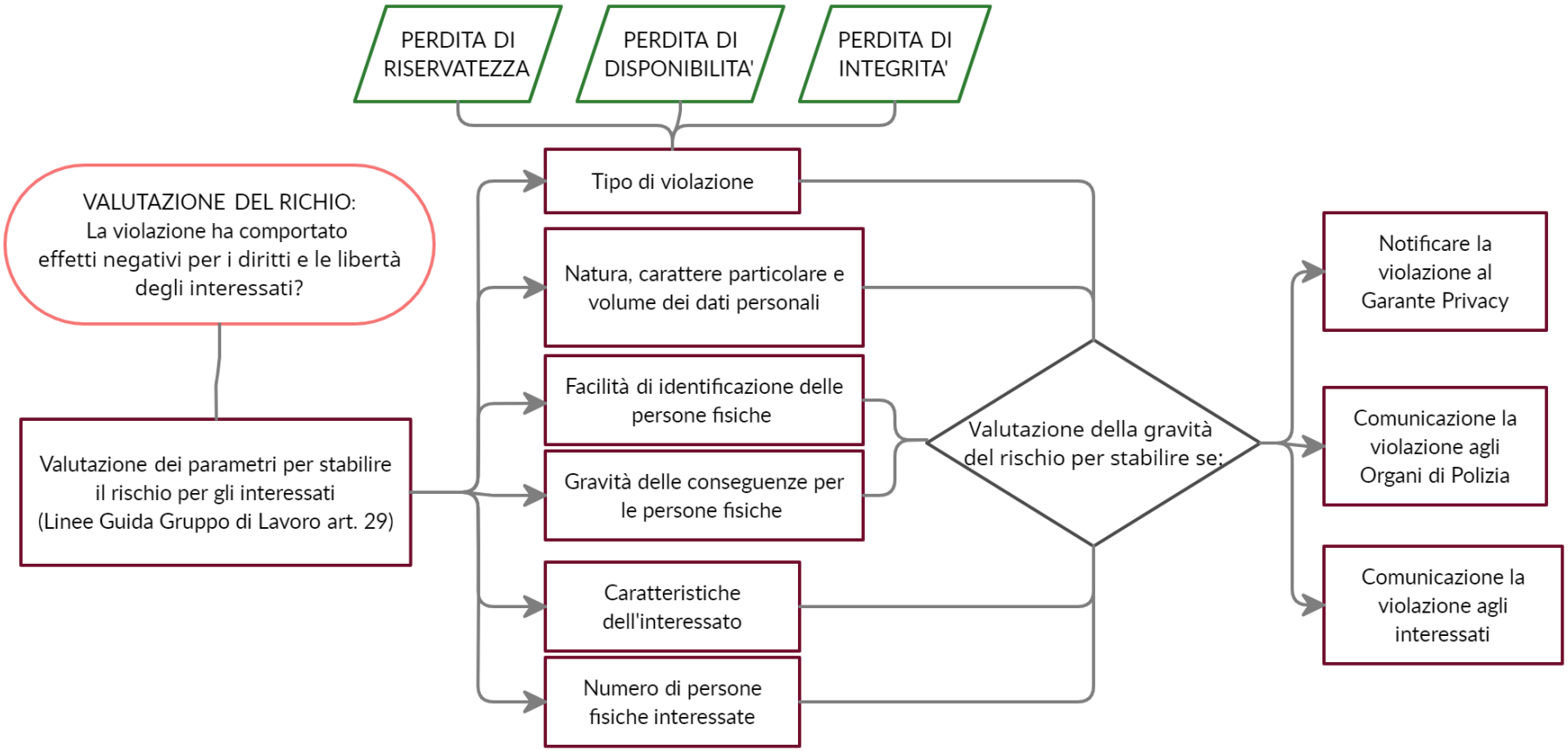
In base al rischio derivante dalla violazione dei dati il Responsabile, insieme al DPO, valuta se:

- 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 (la comunicazione può essere anticipata nella fase preliminare anche se l'evento non ha determinato una violazione dei dati).

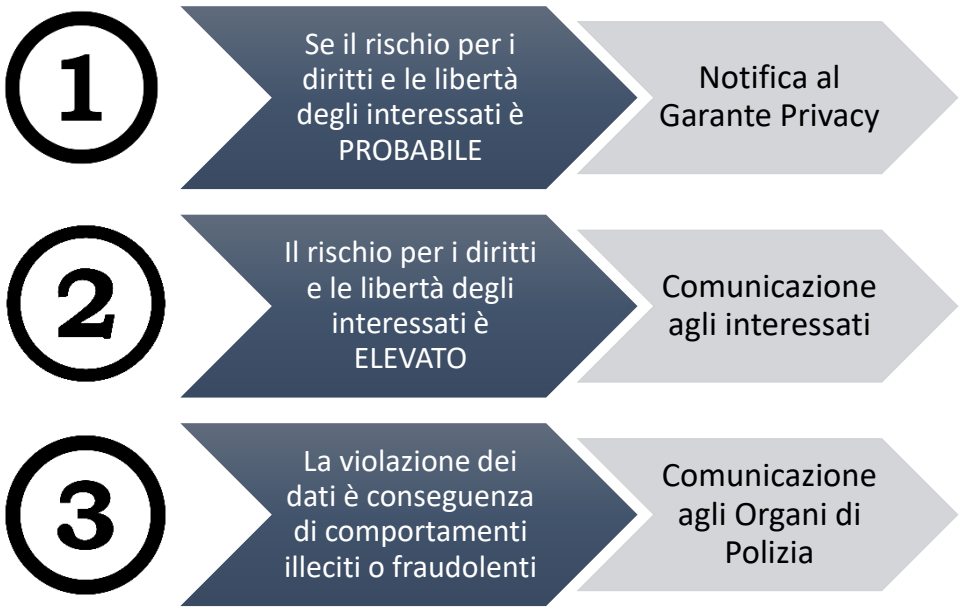
Di seguito il link di collegamento allo strumento di autovalutazione messo a disposizione dal Garante Privacy per individuare le azioni da intraprendere a seguito di una violazione dei dati derivante da un incidente di sicurezza: https://servizi.gpdp.it/databreach/s/self-assessment

In ogni caso, anche se non si effettuano notifiche e comunicazioni, è necessario **inserire la segnalazione all'interno del Registro degli incidenti di sicurezza e violazioni dei dati (c.d. Data Breach)** (Allegato 3) conservato nella cartella "PRIVACY → Policy e Procedure Privacy → Procedura di gestione delle violazioni dei dati", condivisa all'interno di Quattrozeta s.r.l.

SCHEMA DELLA FASE 2 RELATIVA ALLA GESTIONE DELLA SEGNALAZIONE E VALUTAZIONE DEL RISCHIO



FASE 3 – NOTIFICA AGLI ORGANI COMPETENTI E COMUNICAZIONE AGLI INTERESSATI



Tali attività sono gestite dal Responsabile che ha segnalato la violazione dei dati e valutato il rischio derivante con il supporto del DPO. Per alcune di queste attività potrà essere, inoltre, coinvolto l'Amministratore Unico in quanto Legale Rappresentante.

① La **Notifica al Garante per la Protezione dei Dati Personali** dovrà seguire le indicazioni riportate sul sito internet istituzionale dell'Autorità alla sezione "ACCEDI AL SERVIZIO TELEMATICO DEDICATO AL DATA BREACH" => COMPILAZIONE DELLA NOTIFICA disponibile al seguente link: https://servizi.gpdp.it/databreach/s/.

TERMINI TEMPORALI PER LA PRESENTAZIONE DELLA NOTIFICA

La notifica dev'essere eseguita **senza ingiustificato ritardo e, ove possibile, entro 72 ore** dal momento in cui il Responsabile del procedimento ha preso in carico la segnalazione, compilando la scheda di gestione (FASE 1), inviandola all'email dell'Amministratore Unico e del DPO, per l'attivazione della procedura di Violazione dei dati. Le notifiche al Garante Privacy effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.

La procedura di notifica di una violazione dei dati, prevista dal Garante Privacy, prevede che la stessa sia effettuata dal Rappresentante Legale del Titolare del trattamento o da un altro soggetto che agisce su sua delega, assumendosi la responsabilità circa la veridicità delle informazioni fornite.
Non è necessario allagare l'atto di delega ma è sufficiente indicare che la notifica viene presentata in qualità di delegato del rappresentante legale specificandone il cognome e nome.

Inoltre, la procedura richiede di indicare i dati di contatto del Responsabile della Protezione dei Dati (c.d. DPO) ed, in particolare, il numero di protocollo assegnato alla comunicazione dei dati di contatto effettuata al Garante Privacy di seguito riportato: **20180050143.**

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 che ha seguito l'analisi della violazione o altro punto di contatto;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui la Quattrozeta s.r.l. 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 La **Comunicazione o denuncia agli Organi di Polizia** sarà effettuata dal Responsabile che ha seguito l'analisi della violazione o, in alternativa, dal Legale Rappresentante.
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/.
La comunicazione può essere anticipata alla fase preliminare di gestione dell'incidente di sicurezza anche se l'evento non ha determinato una violazione dei dati.

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 disposizioni pervenute ed il presente documento e/o i suoi allegati potranno essere modificati anche in tempi successivi.

Allegato 1 - Scheda di segnalazione - “PROCEDURA DI VIOLAZIONE DEI DATI - DATA BREACH”

	SCHEDA DI SEGNALAZIONE "PROCEDURA DI VIOLAZIONE DEI DATI - DATA BREACH"	PAG. **17/23**

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 Quattrozeta S.r.l. mette a disposizione la presente scheda per segnalare tali eventi. Qualora gli spazi del modulo non siano sufficienti è possibile allegare documenti integrativi.

INDICAZIONI OPERATIVE **PER L'INVIO DELLA SEGNALAZIONE:**	Al termine della compilazione della sezione A "Compilazione a cura del segnalante" è necessario: Inviare il modulo a mezzo e-mail: privacy@quattrozeta.it OPPURE • Consegna il modulo a mano presso gli Uffici Amministrativi in Via G. Maggi, 3 – Novara, 28100

A) COMPILAZIONE A CURA DEL SEGNALANTE

DATI RELATIVI AL **SEGNALANTE**	Cognome/Nome	……
	Num. di telefono	……
	Qualifica	☐ Dipendenti/collab. ☐ Interessato ☐ Altro ……

DESCRIZIONE DELL'EVENTO

Circostanze in cui ci si è accorti dell'evento

Data ……/……/…… ed orario …… in cui ci si è accorti dell'evento oggetto di segnalazione

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; famigliari; operatori; soggetti terzi)
- Numero di persone coinvolte dalla violazione (i dati erano relativi ad una sola persona oppure a n°___ di 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 dal segnalante: ☐ No ☐ Sì, specificare quali:

……

……

……

Data compilazione del presente modulo: ……/……/……

Firma segnalante: ……

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

	**TITOLARE DEL TRATTAMENTO**
	Il Titolare del trattamento è Quattrozeta S.r.l. (P. IVA 02040460038) con sede in Via G. Maggi, 3 – Novara, 28100, telefono 03211828128, e-mail: info@quattrozeta.it, PEC: quattrozeta@pec.it
	**RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (c.d. DPO)**
	Il DPO nominato è contattabile presso Labor Service S.r.l., con sede in via A. Righi n. 29, 28100 Novara (NO); telefono: 0321.1814220; e-mail: privacy@labor-service.it; PEC: pec@pec.labor-service.it
	**FINALITÀ E BASI GIURIDICHE DEL TRATTAMENTO**
	I dati anagrafici e di contatto del soggetto segnalate conferiti con il presente modulo saranno trattati, con modalità prevalentemente informatiche e telematiche, per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e s.m.i.), in particolare per dar corso alla segnalazione ed effettuare tutte le verifiche richieste dall'art. 33 GDPR anche attraverso il contatto con il segnalate. 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.
	**DESTINATARI DEI DATI**
	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 e all'effettuazione di tutte le verifiche necessarie per l'analisi della violazione dei dati. 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.
	**PERIODO DI CONSERVAZIONE DEI DATI**
	I dati personali raccolti sono conservati per il periodo necessario per adempiere alle finalità di cui sopra ed in conformità a disposizioni normative.
	**DIRITTI DELL'INTERESSATO**
	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). I diritti possono essere esercitati mediante comunicazione attraverso i dati di contatto di cui sopra. Inoltre, l'interessato ha il diritto di proporre reclamo ad un'autorità di controllo (Garante per la protezione dei dati personali: https://www.garanteprivacy.it/modulistica-e-servizi-online/reclamo).

Allegato 2 – Scheda di gestione - “PROCEDURA DI VIOLAZIONE DEI DATI - DATA BREACH”

	SCHEDA DI GESTIONE "PROCEDURA DI VIOLAZIONE DEI DATI - DATA BREACH" Gestione della violazione dei dati personali	**PAG. 1/2**

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, Quattrozeta s.r.l. mette a disposizione la presente Scheda per segnalare gli eventi che hanno determinato una "violazione di dati", secondo la "Procedura Gestione delle violazioni dei dati - Data Breach".

FASE 1 - AVVIO DELLA PROCEDURA DI DATA BREACH
Compilazione a cura del Segnalante

INDICAZIONI OPERATIVE PER L'INVIO DELLA SEGNALAZIONE	Al termine della compilazione della FASE 1 della presente Scheda inviare il modulo con oggetto "SEGNALAZIONE VIOLAZIONE DATI" a: • email dedicata alla segnalazioni: privacy@quattrozeta.it • email del DPO: privacy@labor-service.it	
UFFICIO	……	
NOME RESPONSABILE	Cognome/Nome	……

SOGGETTI COINVOLTI NELL'ATTIVITÀ DI ANALISI

Il Responsabile ha coinvolto per l'analisi dell'evento:
❑ Amministratore di Sistema: …….. ❑ Responsabile del trattamento ……..
❑ Personale autorizzato al trattamento…… ❑ Altro: ……
Indicare eventuali dati di contatto: ……

ANALISI

Descrizione dell'incidente di sicurezza che ha determinato la violazione comprensivo dei termini temporali dell'evento:

Descrizione delle attività di analisi e indicazione delle misure di sicurezza tecniche e organizzative applicate prima dell'evento segnalato ed eventuali interventi adottati dopo l'evento:

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)

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

Specificare la tipologia e numero di dati e la categoria e numero di interessati coinvolti:

Eventuali allegati:

INFORMAZIONI SUL TRATTAMENTO DEI DATI ai sensi dell'art.13 Regolamento (UE) 2016/679: Il TITOLARE del trattamento è la Quattrozeta s.r.l. Il DPO è reperibile alla e-mail: privacy@labor-service.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). 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 Privacy 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 Responsabile: ……

FASE 2 - GESTIONE DELLA SEGNALAZIONE E VALUTAZIONE DEL RISCHIO

Compilazione a cura del Responsabile competente
con il supporto del DPO ed eventuali ulteriori soggetti coinvolti

RESPONSABILE	Cognome/Nome	……

VALUTAZIONE DEL RISCHIO

❑ **Non ci sono potenziali effetti negativi per i diritti e le libertà degli 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;
- ❑ Pregiudizio alla reputazione
- ❑ Conoscenza da parte di terzi non autorizzati;
- ❑ Decifratura non autorizzata della pseudonimizzazione;
- ❑ Perdita di riservatezza dei dati personali protetti da segreto professionale;
- ❑ Qualsiasi altro danno economico o sociale significativo (specificare) ……

Stima della gravità della violazione: ❑ Trascurabile ❑ Basso ❑ Medio ❑ Alto
Specificare:

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

FASE 3 - NOTIFICA AGLI ORGANI COMPETENTI E COMUNICAZIONE AGLI INTERESSATI

Compilazione a cura del Responsabile competente
con il supporto del DPO, ed eventualmente dell'Amministratore Unico

ALLA LUCE DELLE ANALISI E DELLE VALUTAZIONI SVOLTE SI DECIDE DI:

❑ Notificare la violazione al Garante Privacy ❑ NON Notificare la violazione al Garante Privacy
Specificare:

❑ Dare comunicazione agli Organi di Polizia ❑ NON dare comunicazione agli Organi di Polizia
Specificare:

❑ Dare comunicazione ai soggetti interessati ❑ NON dare comunicazione ai soggetti interessati
Specificare:

Data di termine compilazione: ……../……../……

Firma del Responsabile: ……

Firma dell'Amministratore Unico: ……

Firma per presa visione del DPO: ……

Allegato 3 – Registro Incidenti di sicurezza & Violazione dei dati (c.d. Data Breach)

mediaterraneo
PROMOZIONE E SVILUPPO TURISTICO

REGISTRO INCIDENTI DI SICUREZZA & VIOLAZIONI DEI DATI (c.d. DATA BREACH)

EVENTO					Totale Data Breach		0	Totale Notifiche al GARANTE PRIVACY		0	Totale Comunicazioni agli interessati		0	
Ricezione della segnalazione (Data - orario) e n° codice segnalazione	**Soggetti coinvolti nell'attività di analisiIncidente di sicurezza (SI/NO)**	**E' solo un incidente di sicurezza? (SI/NO)**	**Ruolo Privacy** (Titolare/Contitolare /Responsabile/Altro)	**Breve descrizione dell'evento e dell'analisi svolta**	**E' data breach? (SI/NO)**	**Causa della violazione** (accidentale o dolosa/esterna o interna)	**Natura della violazione** (perdita di riservatezza/integrità/disponibilità	**Potenziali effetti negativi per i diritti o le libertà degli interessati** (es. Perdita del controllo dei dati personali;Limitazione dei diritti; Discriminazione; furto; frode ecc)	**Stima della gravità** (Trascurabile/Basso/Medio/Alto)	**Azioni correttive messe in atto**	**Notifica al Garante Privacy (SI/NO)**	**Comunicazione agli organi di Polizia (SI/NO)**	**Comunicazione agli interessati (SI/NO)**	**Note**