PROCEDURA OPERATIVA INTERNA DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

INDICE

PREMESSA

Il Regolamento UE 2016/679 sulla Privacy in materia di Protezione dei Dati Personali (General Data Protection Regulation "GDPR") introduce la necessità di adottare un **processo di gestione degli incidenti con impatto sui dati personali trattati**.

Tale tipologia di incidente si configura come una **violazione di sicurezza** che comporta, accidentalmente o in modo illecito, la distruzione o la perdita permanente, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Una violazione, pertanto, può avere un insieme di effetti negativi, anche significativi, sugli individui e può comportare, ad esempio:

- ***La perdita di controllo sui propri dati personali;***
- ***La limitazione dei diritti dell'interessato;***
- ***La discriminazione;***
- ***Il furto d'identità o la frode;***
- ***La perdita finanziaria;***
- ***Il danno reputazionale;***
- ***La perdita di riservatezza dei dati personali protetti da segreto professionale;***
- ***Qualsiasi altro svantaggio economico o sociale rilevante.***

1. SCOPO

Scopo della presente **Procedura Operativa interna** è quello di descrivere il processo di gestione degli incidenti di sicurezza, nel contesto delle procedure definite dalla società con particolare riferimento alle violazioni di dati personali, nell'ambito dei **servizi informatici e della sicurezza fisica.**
La società, con la presente Procedura Operativa ed i documenti in essa richiamati, definisce inoltre i **ruoli e relative responsabilità** nella gestione degli eventuali incidenti e violazioni di dati personali o Data Breach.

2. AMBITO DI APPLICAZIONE

La Procedura si applica all'intera struttura della **CASA LIVORNO E PROVINCIA SPA** (di seguito anche solo Società) con particolare riferimento al personale che svolge trattamenti di dati personali.

3. RIFERIMENTI NORMATIVI

La Procedura considera i seguenti riferimenti normativi:

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (General Data Protection Regulation - GDPR);
- D.Lgs. 196/ 2003 - Codice in materia di protezione dei dati personali;
- Provvedimenti Garante per la protezione dei dati personali;
- Provvedimenti del Comitato Europeo per la Protezione dei Dati (European Data Protection Board – EDPB);
- Linee guida Garante Italiano per attuazione del Regolamento Europeo (GDPR);
- Linee guida del Gruppo di lavoro Articolo 29 (WP 29).

4. TERMINI E DEFINIZIONI

Acronimo/ Definizione	**Descrizione**
GDPR	Regolamento UE 2016/679, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Nella sua formulazione originale in lingua inglese: "General Data Protection Regulation".
WP29	Gruppo di lavoro istituito dall'art. 29 della direttiva 95/46 come organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno

	Stato membro, dal GEPD (Garante Europeo della Protezione dei Dati), nonché da un rappresentante della Commissione.
Autorità di Controllo competente	Autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 del GDPR e competente ai sensi del successivo art. 55. Per i trattamenti effettuati in uno stabilimento principale avente sede in Italia, l'Autorità Garante per la Protezione dei dati personali è l'Autorità di Controllo Competente.
Data Breach o Violazione di dato personale	Una violazione della sicurezza che porta a distruzione, perdita, alterazione, divulgazione non autorizzata o accesso non autorizzato a dati personali trasmessi, archiviati o altrimenti elaborati.
DPO	Data Protection Officer o Responsabile della protezione dati.
TRV	Team di Risposta alle Violazioni

5. CRITERI GENERALI

Un **incidente di sicurezza** è evento osservabile all'interno di un contesto predefinito che si discosta dalla normale operatività delle strutture o dei sistemi, che potrebbe determinare conseguenze negative.
Si considera violazione dei dati personali (nel proseguo anche "Incidente Privacy" o "Data Breach") **qualunque evento che comprometta, anche in maniera del tutto accidentale, la sicurezza dei dati personali trattati in qualsiasi formato** (ad es., elettronico o cartaceo) e di conseguenza i diritti e le libertà degli interessati. La violazione dei dati personali comprende almeno i casi per i quali si rimanda al paragrafo 6.8 "Tassonomia degli incidenti privacy" della Procedura.
Sulla base della definizione introdotta e in coerenza con quanto definito nelle linee guida emesse dal WP29 (rif. WP250 - "Guidelines on Personal data breach notification under Regulation 2016/679") le violazioni possono essere classificate in base ai seguenti tre principi sulla sicurezza delle informazioni:

- **"Violazione della Riservatezza",** in caso di divulgazione o accesso, accidentale o comunque non autorizzato, di dati personali;
- **"Perdita di Disponibilità"**, in caso di perdita o distruzione permanente, accidentale o comunque non autorizzata, dei dati personali;
- **"Violazione dell'Integrità"**, in caso di alterazione, accidentale o comunque non autorizzata, dei dati personali.

Limitatamente ai temi di disponibilità e integrità, la Società identifica i casi di applicabilità dei data breach agli eventi che comportino una compromissione irreversibile di tali caratteristiche del dato personale.
Le possibili violazioni possono interessare una o più delle tipologie sopra elencate contemporaneamente.

5.1 NOTIFICA ALL'AUTORITÀ DI CONTROLLO (ART. 33 GDPR)

Il Titolare del trattamento deve notificare la violazione dei dati personali all'Autorità di controllo competente, coinvolgendo il Responsabile della protezione dei dati (DPO) ***Avv. Gian Luca***

Zingoni, **"*senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza*" (rif. art. 33.1 GDPR).**
Ciò non risulta applicabile nel momento in cui il Titolare dimostri, in accordo al principio di ***accountability***, che la violazione non comporta rischi per i diritti e le libertà degli interessati.
Qualora tale notifica avvenga oltre il termine delle 72 ore, il Titolare **deve** corredare la notifica con **le ragioni del ritardo**; è inoltre possibile condurre la cosiddetta "*notification in phases*" in cui, dopo una prima notifica, ulteriori informazioni possono essere fornite in fasi successive.
La notifica della violazione dei dati personali all'Autorità di controllo competente deve almeno contenere:

- La descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali impattati;
- Il nome e i dati di contatto del referente interno nominato per la materia Dr. Matteo Guidi e del DPO (Avv. Gian Luca Zingoni), e di ogni altro soggetto di riferimento all'interno della Società presso cui ottenere maggiori informazioni;
- Le probabili conseguenze della violazione dei dati personali;
- Le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

5.2 COMUNICAZIONE AGLI INTERESSATI (ART. 34 GDPR)

Qualora la violazione dei dati sia suscettibile di presentare **un rischio elevato** (rif. art. 34.1) per i diritti e le libertà della persona fisica, è necessario informare tempestivamente gli interessati stessi, al fine di consentire loro di prendere le precauzioni necessarie.

Le comunicazioni agli interessati devono essere effettuate non appena possibile (si veda par. 6.6.1.2 **"Comunicazione verso gli Interessati"**).
Per stabilire la necessità di comunicazione agli interessati, in caso di violazione dei dati, la normativa descrive i seguenti fattori utili per valutare i rischi per i diritti e le libertà delle persone fisiche:

- Se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- Se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- Se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- In caso di valutazione di aspetti personali, in particolare mediante l'analisi/previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le

preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- Se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
- Se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Il livello di rischio, per i diritti e le libertà dell'interessato, deve essere:

- Determinato con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento;
- Considerato in base ad una valutazione il più possibile oggettiva mediante cui si stabilisce se la violazione dei dati rilevati possa comportare un rischio (solo comunicazione al Garante) o un rischio elevato (comunicazione al Garante e agli interessati).

La comunicazione verso gli interessati non è richiesta qualora sia valida una delle seguenti condizioni:

A. Sono state messe in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
B. Sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
C. Detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

5.3 INVENTARIO DELLE VIOLAZIONI DI DATI PERSONALI (ART. 33.5 GDPR)

A seguito del principio di responsabilizzazione, prescritto dalla normativa, la Società deve inoltre documentare qualsiasi violazione di dati personali subita, anche se non notificate all'autorità di controllo competente e non comunicate agli interessati, nonché le relative circostanze e conseguenze nonché i provvedimenti adottati.

La Società quindi tiene traccia nell'inventario delle violazioni, indipendentemente dalle notifiche e/ o comunicazioni che possono essere eseguite in seguito alla violazione dei dati, documentando le valutazioni a supporto delle decisioni prese in risposta a una violazione. In particolare, se una violazione non viene notificata all'autorità di controllo competente, deve essere redatta la relativa giustificazione a supporto di tale decisione, includendo i motivi per i quali la violazione in questione non sia stata ritenuta una potenziale causa di rischi per i diritti e le libertà degli individui. Analogamente, se il Titolare decide di non comunicare una violazione agli interessati (rif. Art. 34.3 GDPR), è necessario che si fornisca prova adeguata della sussistenza delle condizioni prescritte che portano a valutare che la violazione non arrechi rischi elevati alle persone fisiche.

6. PROCESSO DI GESTIONE DEGLI INCIDENTI PRIVACY

Sulla base di quanto sopra, **CASALP SPA** definisce la presente procedura che descrive le disposizioni, i principi e i dettagli in merito all'approccio strutturato per la gestione degli incidenti privacy, a partire dall'analisi degli impatti che gli stessi possono comportare a diritti e libertà degli interessati, fino alla conseguente gestione delle eventuali comunicazioni verso autorità di controllo competente e interessati entro le tempistiche prestabilite.
Il processo di gestione degli incidenti privacy si articola nelle fasi sotto riportate:

- **Rilevazione**: in cui l'incidente di sicurezza viene rilevato o comunque segnalato alla Società;
- **Costituzione del Team**: in cui si costituisce il **Team di Risposta alle Violazioni (TRV)**;
- **Gestione tecnica, registrazione e analisi**: in cui si gestisce tecnicamente l'incidente e si raccolgono quante più informazioni di dettaglio sull'evento e sulla potenziale violazione;
- **Classificazione e analisi**: l'incidente viene classificato quale violazione dei dati personali e viene registrato nel relativo registro;
- **Valutazione degli impatti verso gli interessati**: in cui si valutano gli impatti e i rischi della violazione per i diritti e le libertà degli interessati, nonché le eventuali attività di notifica e comunicazione da effettuare;
- **Notifiche e comunicazioni:**
  - **Notifica all'Autorità di Controllo competente**: in cui si dichiarano specifiche informazioni sulla violazione occorsa;
  - **Comunicazione verso gli interessati**: in cui si definisce e si implementa la strategia di comunicazione verso l'interessato della violazione occorsa;
- **Registrazione della chiusura dell'evento**: in cui si inserisce il termine della procedura, nonché i relativi esiti e le operazioni effettuate;
- **Monitoraggio delle misure di sicurezza** - in cui si gestisce e si tiene monitorato, in modo preventivo e pro-attivo, il livello di efficacia delle previste misure di sicurezza sia di natura fisica che in ambito ICT.

Nel caso la Società agisca quale Responsabile del trattamento, ad esempio nell'ambito di un trattamento di dati personali **per conto di una società controllata**, la Società deve supportare il Titolare nell'applicazione dei propri doveri secondo quanto definito dalla Procedura.

6.1 RILEVAZIONE

In questa fase si acquisisce la **notizia di un incidente di sicurezza**, che potrebbe determinare una possibile violazione sui dati personali, ovvero rientrare nell'ambito di applicazione della Procedura.
Tale fase del processo si differenzia a seconda della **natura dell'evento**; si distinguono Incidenti di

1. **"ICT Security"**
2. **"Sicurezza Fisica".**

6.1.1 RILEVAZIONE IN AMBITO ICT SECURITY

Il processo di rilevazione degli incidenti di sicurezza ICT, che possono potenzialmente configurarsi come Data Breach, è demandato in prima istanza all'amministratore del sistema informatico, come

da Provvedimento del garante per la protezione dei dati personali "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008, così come modificato in base al provvedimento del 25 giugno 2009.
L'identificazione degli eventi può derivare da:

- **Evidenze derivanti da sistemi di monitoraggio (log, alert);**
- **Allarmi da sistemi antimalware o anti-intrusione;**
- **Controllo e analisi periodica del software o della banca dati;**
- **Segnalazione degli utenti del software o della banca dati, ovvero dipendenti o collaboratori;**
- **Segnalazione da parte degli interessati;**
- **Possibili problematiche derivanti da migrazione software, applicazione di upgrade o aggiornamenti;**
- **Notizie di vulnerabilità dei sistemi in uso;**
- **Possibili problematiche derivanti da guasti, interruzioni di servizio e malfunzionamenti.**

6.1.2 RILEVAZIONE IN AMBITO SICUREZZA FISICA

Il processo di gestione degli eventi relativi alla sicurezza **fisica** è demandato invece **al Consiglio di Amministrazione**, per il tramite del Dirigente/Responsabile dell'Area coinvolta.
A titolo esemplificativo si propongono alcuni casi di tali fattispecie:

- Furto di dispositivi ICT (ad es., laptop, desktop, dispositivi di memorizzazione, etc);
- Incendio o allagamento degli archivi fisici documentali;
- Effrazione dei locali in cui sono custoditi o gestiti archivi di documenti cartacei che contengono dati personali (ad es. archivi documentali, locali in cui sono custodite le cartelle sanitarie dei dipendenti, etc.);
- Furto di faldoni cartacei.

Qualora le telecamere anti-effrazione situate al perimetro dell'azienda abbiano registrato dei movimenti che possano lasciar pensare ad una qualsiasi violazione fisica dei locali aziendali, il responsabile dell'impianto di video registrazione dovrà tempestivamente comunicare al referente interno, ed in caso di sua assenza direttamente al DPO, l'evento registrato.
Qualora vi sia incidenza (anche solo potenziale) sugli asset informatici è necessario comunicare l'evento immediatamente anche al Dirigete/Responsabile dei Sistemi Informativi ed all'Amministratore del sistema informatico per i dovuti interventi.

6.1.3 SEGNALAZIONE DA PARTE DI RESPONSABILI DEL TRATTAMENTO O TERZE PARTI

La segnalazione di un evento con potenziale impatto sui dati personali può pervenire anche da soggetti terzi ed in particolare dai Responsabili del Trattamento nominati, quali soggetti esterni alla Società che eseguono interamente o parzialmente trattamenti per conto della stessa.

I Responsabili del Trattamento, anche secondo quanto definito contrattualmente, interfacciandosi col Referente Interno Dr. Matteo Guidi, **devono segnalare l'evento senza ingiustificato ritardo**, ove l'evento possa comportare possibili violazioni dei dati personali trattati nell'ambito delle attività svolta.
Il Referente Interno Dr. Matteo Guidi è tenuto a darne immediata comunicazione al Consiglio di Amministrazione ed al DPO Avv. Gian luca Zingoni
La segnalazione proveniente dall'esterno potrà anche essere ricevuta dal personale interno, il quale dovrà inoltrare immediatamente la comunicazione al proprio Dirigente/Responsabile di Area. Quest'ultimo trasmetterà immediatamente e senza ritardo a sua volta la comunicazione al Referente Interno Dr. Matteo Guidi per la gestione.

6.2 COSTITUZIONE DEL TEAM

A seguito della segnalazione, ovvero della rilevazione dell'incidente di sicurezza, al fine di procedere con efficienza e tempestività, **si procede alla costituzione del Team di Risposta alle Violazioni (TRV),** che prevede il coinvolgimento di più soggetti, anche in relazione alla natura dell'evento.
Per gli incidenti in ambito **ICT Security**, il **coordinatore** dell'evento è il Dirigente/Responsabile dei Sistemi Informativi coadiuvato dall'Amministratore del sistema informatico.
Per gli incidenti in ambito di Sicurezza Fisica, il **coordinatore** dell'evento sarà il Consiglio di Amministrazione per il tramite del referente Interno Dr. Matteo Guidi.
I coordinatori, a prescindere dalla natura dell'evento, devono immediatamente contattare:

- Il personale necessario per la gestione dello specifico incidente (ove necessario, anche esterno alla società);
- Il Referente Interno Privacy Dr. Matteo Guidi;
- Il Dirigente Responsabile delle Risorse Umane;
- Il Dirigente Responsabile dell'Area coinvolta
- Il Dirigente Responsabile dell'Area Legale.

6.3 GESTIONE TECNICA, REGISTRAZIONE E ANALISI

L'intervento del **TRV**, tramite gli operatori, permette di identificare la **strategia più idonea al contenimento,** ovvero al porre rimedio agli effetti negativi relativi all'incidente, nonché alla raccolta delle informazioni che risulteranno necessarie nelle successive fasi.
Risulta necessario rilevare almeno le seguenti informazioni relative all'evento:

A. Quando si è verificato;
B. Dove si è verificato (anche in relazione ai sistemi IT);
C. Quale è la presunta fonte;
D. Quali interventi sono stati effettuati a seguito dell'incidente;
E. Chi sono i soggetti coinvolti (ad es. personale amministrativo, operativo, terze parti);
F. Che genere di violazione è occorsa (ad es. disponibilità, integrità, riservatezza, ovvero combinazioni di queste);
G. Quanti dati sono stati coinvolti;
H. Di che natura sono i dati coinvolti (ad es. dati personali, dati generici non personali, ecc.).

La determinazione delle informazioni di cui al punto H determina l'immediato passaggio alla fase successiva. Fatta salva comunque la necessità di raccogliere comunque le informazioni di cui ai punti da A. a G.
In ogni caso, le informazioni raccolte devono essere **REGISTRATE** nel relativo Inventario delle Violazioni, anche in assenza di certezza sulla natura dei dati coinvolti.
La raccolta di queste informazioni, nonché la determinazione della natura dei dati coinvolti nell'evento, sono determinanti al fine della successiva fase di classificazione e analisi.

6.4 CLASSIFICAZIONE E ANALISI

La natura dei dati coinvolti è determinante per la prosecuzione della presente procedura.
Nel caso in cui non si riscontri il coinvolgimento di dati personali è necessario mantenere monitorata la gestione dell'evento, fino alla definitiva chiusura, anche al fine di poter intervenire prontamente in caso di errata valutazione riguardo la natura dei dati violati. Invece, ove si riscontri la violazione di dati personali è necessario procedere all'approfondimento dell'analisi precedentemente svolta.
Resta inteso, che da questo momento decorrono le **72 ore per procedere alla notifica all'Autorità di Controllo competente**.
Pertanto, in caso di violazione dei dati personali è necessario raccogliere le seguenti informazioni relative all'evento:

I. Quanti sono gli interessati coinvolti;
J. Qual è la nazionalità degli interessati;
K. La categoria dei dati personali (ad es. comuni, particolari, giudiziari);
L. Quanti sono i dati per interessato che sono stati coinvolti;
M. Qual è la facilità di identificazione dell'interessato in relazione ai dati;
N. Qual è l'estensione geografica dell'evento;
O. Quali misure tecniche erano già state applicate ai dati oggetto della violazione (ad es. cifratura, pseudonimizzazione, ecc.).

Queste informazioni, oltre che alle informazioni raccolte nella precedente fase, saranno necessarie al fine di valutare l'impatto per i diritti e le libertà degli interessati.
Nel caso in cui la Società tratti i dati coinvolti in qualità di Responsabile del trattamento, il Referente Interno Privacy, deve coinvolgere il Titolare del trattamento, anche tramite il DPO.

6.5 VALUTAZIONE DEGLI IMPATTI VERSO GLI INTERESSATI

In questa fase il coordinamento dell'evento, ad eccezione degli ulteriori interventi tecnici necessari, è di responsabilità del **Referente Interno Privacy Dr. Guidi Matteo**, il quale, coadiuvato dalle altre parti del TRV compila il documento di valutazione dell'impatto che permette di eseguire una stima del livello di impatto complessivo dell'evento per i diritti e le libertà dell'interessato, secondo una scala a 3 livelli (Basso, Medio, Alto).
Le metriche introdotte consentono di classificare come "Basso" il livello di rischio per tutti gli eventi che, pur potendo formalmente presentare caratteristiche di violazione ai dati personali, non configurano in alcun modo pregiudizio per i diritti e le libertà degli interessati e per i quali non si reputa necessaria alcuna comunicazione, né verso il Garante né verso gli interessati stessi.
Il TRV, sentiti tutti i sui componenti, esprime la propria valutazione sulla violazione occorsa:

- In caso di "Basso" livello di rischio, non si procede alla notifica e si annota la decisione, corredata dalle motivazioni nel registro delle violazioni;
- In caso di livello di rischio "Medio" o "Alto", si procede alla fase di notifica.

Se il TRV, anche coinvolgendo eventualmente ulteriori funzioni, tecnici e consulenti – anche esterni alla Società - non riuscisse a valutare l'impatto della violazione entro 48 ore dall'acclarato coinvolgimento di dati personali, anche per mancanza di informazioni, si deve procedere con:

- Un'analisi di impatto che prenda in considerazione il caso peggiore;
- Una comunicazione verso l'Autorità garante che verrà successivamente rettificata o cancellata se necessario.

Al termine di questa fase il TRV:

- Procede immediatamente - in caso di livello di rischio stimato "medio" o "alto" – all'attivazione delle necessarie ed ulteriori contromisure per la mitigazione del rischio, delegando le operazioni alla struttura tecnica competente, che deve informare costantemente il TRV dei risultati dell'azione di mitigazione del rischio e di eventuali ulteriori elementi che possano comportare una diversa valutazione d'impatto;
- Procede alla fase di notifica all'Autorità di Controllo competente e, ove ritenuto necessario, alla comunicazione verso gli interessati.

Come accennato, in ogni caso, la violazione dovrà essere registrata all'interno dell'inventario delle violazioni da parte del **Referente Interno Privacy, che ha la responsabilità di mantenere tale inventario.**
Nel caso in cui la Società sia Responsabile del Trattamento, il TRV deve comunicare la valutazione al Titolare del Trattamento, anche tramite il DPO.

6.6 NOTIFICHE E COMUNICAZIONI

6.6.1 AZIENDA IN QUALITA' DI TITOLARE DEL TRATTAMENTO

Come meglio espresso al paragrafo 5, sul Titolare del trattamento, a seguito della analisi e valutazione dell'incidente di sicurezza che coinvolga dati personali, ricade l'obbligo di notifica dell'evento.
A seconda della gravità dell'evento, come meglio esplicitato nei successivi paragrafi, il Titolare del trattamento notifica la violazione dei dati personali all'autorità di controllo competente (6.6.1.1) e, nei casi ritenuti più gravi, anche all'interessato (6.6.1.2).

6.6.1.1 NOTIFICA ALL'AUTORITA' DI CONTROLLO

In questa fase la Società, a seguito dei risultati dell'analisi e valutazione da parte del TRV che abbia individuato un rischio Medio o Alto e di concerto con la Direzione aziendale, attraverso il Referente Interno Privacy, notifica all'Autorità di Controllo competente**, entro 72 ore dalla rilevazione**, la violazione stessa attraverso il "Modello segnalazione Data Breach".
La comunicazione verso l'Autorità di Controllo competente deve contenere almeno le seguenti informazioni:

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

6.6.1.2 COMUNICAZIONE VERSO GLI INTERESSATI

In questa fase la Società, a seguito dei risultati dell'analisi e valutazione da parte del TRV che abbia individuato un rischio Alto e di concerto con la Direzione aziendale, attraverso il Referente Interno Privacy, comunica agli interessati la violazione dei dati personali.
La comunicazione agli interessati non sarà eseguita se:

- La Società ha applicato adeguate misure tecniche e organizzative per proteggere i dati personali prima della violazione, in particolare quelle misure che rendono incomprensibili i dati personali a chi non è autorizzato ad accedervi (ad es. crittografia);
- Subito dopo una violazione, la Società ha preso provvedimenti per assicurare che l'elevato impatto sui diritti e la libertà degli interessati non sia più applicabile (ad es. il furto di dotazioni informatiche sia stato individuato prima che le informazioni siano state utilizzate e la loro memoria è stata cancellata da remoto).

Analogamente alla notifica verso l'Autorità di Controllo competente, la comunicazione verso gli interessati conterrà almeno le seguenti informazioni:

- La descrizione, con un linguaggio semplice e chiaro, della natura della violazione dei dati personali;
- Il nome e i dati di contatto del DPO Avv. Gian Luca Zingoni, o di altro soggetto incaricato all'interno della Società presso cui ottenere più informazioni;
- La descrizione delle probabili conseguenze della violazione dei dati personali;
- La descrizione delle misure adottate o di cui si propone l'adozione da parte della Società per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La modalità di contatto sarà definita sulla base della tipologia di violazione identificata e sulla base degli interessati coinvolti e potrà comprendere, a titolo di esempio:

- Comunicazioni dirette agli interessati (se la Società è in possesso dei loro recapiti);
- Informazioni sul sito istituzionale dell'azienda, in termini di misure di sicurezza implementate dalla Società e misure di sicurezza che gli interessati possono intraprendere, aggiornamenti sullo stato della violazione, strumenti per valutare se si è stati oggetto di violazione;
- Istituzione di un'assistenza tramite call center o tramite live chat richiamabile dal sito istituzionale;
- Comunicati stampa;

- Contenuti multimediali sui social network.

Dovranno inoltre essere previste adeguate modalità di raccolta e risposta di possibili quesiti da parte degli interessati, compreso un possibile canale di comunicazione verso il Settore Legale in caso di contenziosi.

6.6.2 AZIENDA IN QUALITA' DI RESPONSABILE DEL TRATTAMENTO

L'Azienda, ove agisca in qualità di Responsabile del trattamento, è obbligata (art. 33.2 GDPR) a comunicare al Titolare del trattamento eventuali violazioni dei dati personali, senza ingiustificato ritardo. Pertanto, a seguito dell'analisi e della valutazione della violazione, è necessario che renda disponibile, ovvero comunichi in modo qualificato (6.6.2.1), oltre ad un punto di contatto, anche tutte le informazioni necessarie al Titolare, al fine di permettere una corretta valutazione dell'evento e possa adempiere agli obblighi di legge.

6.6.2.1 COMUNICAZIONE VERSO IL TITOLARE DEL TRATTAMENTO

In questa fase, che è alternativa rispetto alle fasi di notifica all'autorità di controllo (6.6.1.1) e comunicazione all'interessato (6.6.1.2), l'Azienda comunica al Titolare:

- La descrizione nel dettaglio la natura della violazione dei dati personali, ivi compresi, ove possibile, le categorie, il numero approssimativo e l'identità degli interessati coinvolti e le categorie e il numero approssimativo di dati personali coinvolti (ove possibile);
- Il nominativo e i dati di contatto del responsabile della protezione dei dati (ove nominato) o altro punto di contatto ove sia possibile ottenere maggiori informazioni;
- La descrizione delle probabili conseguenze della violazione dei dati personali (ove possibile);
- La descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
- L'indicazione se è opportuna o doverosa la notificazione all'Autorità di controllo e/o anche agli interessati coinvolti (ove possibile);
- Ogni altra informazione che possa essere utile al Titolare ai fini della comunicazione della violazione di dati personali all'Autorità di controllo.

Questa comunicazione dovrà essere effettuata mediante l'utilizzo di tecniche che prevedono la riconducibilità della comunicazione al mittente, nonché l'indicazione dell'effettiva ricezione da parte del Titolare (PEC). Inoltre, ove possibile, è preferibile apporre alla comunicazione una firma avanzata, qualificata o digitale, nonché una validazione temporale qualificata (marca temporale).

6.7 GESTIONE DELL'INVENTARIO DELLE VIOLAZIONI

In questa fase il Referente Interno Privacy procede all'aggiornamento dell'Inventario delle Violazioni ("Inventario elenco delle violazioni").
In tale inventario sono contenute le informazioni riguardanti le violazioni occorse, a prescindere dalle eventuali comunicazioni all'autorità di controllo competente o agli interessati.
Ogni evento è descritto, sulla base delle informazioni minime da comunicare all'Autorità di Controllo competente, comprendendo almeno le seguenti informazioni:

- Il Servizio o il responsabile al trattamento che ha eseguito la segnalazione;

- Le modalità di rilevazione;
- Il numero di ticket/incidente collegato (se presente);
- Una breve descrizione dell'evento occorso;
- L'indicazione della data/periodo della violazione e del momento della sua attestazione;
- L'indicazione del luogo in cui è avvenuta la violazione dei dati;
- La tipologia di violazione occorsa e la tipologia di dispositivo oggetto della violazione;
- Una sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti;
- La quantità di dati personali e il numero degli interessati impattati dalla violazione;
- L'indicazione della tipologia dei dati coinvolti nella violazione;
- L'indicazione se la violazione coinvolge interessati che si trovano in altri Paesi UE;
- Il livello di rischio per gli interessati;
- Le misure e i controlli di sicurezza in essere applicati ai dati colpiti da violazione;
- Le misure tecniche ed organizzative assunte per contenere la violazione dei dati e prevenire eventi simili futuri;
- Se effettuata, il contenuto della comunicazione agli interessati e l'indicazione del canale utilizzato per tale comunicazione;
- Laddove la scoperta della violazione non sia stata contestuale al verificarsi dell'evento che l'ha generata, devono essere puntualmente indicate le ragioni che non hanno consentito l'immediata rilevazione dell'evento e le misure adottate o che si intende adottare affinché ciò non si ripeta in futuro.

Se l'evento segnalato non è stato valutato come violazione dei dati personali, saranno annotate le motivazioni che hanno portato a tale tipologia di valutazione.

6.8 TASSONOMIA DEGLI INCIDENTI PRIVACY

La Società, nell'ambito e come guida alla compilazione dell'inventario delle violazioni, ha individuato le tipologie di eventi di seguito riportate:

- ***Distruzione/cancellazione permanente*** - Indisponibilità irreversibile di dati personali trattati con accertata impossibilità di ripristino degli stessi. La violazione può essere relativa ad una eliminazione logica (ad es., cancellazione dei dati) oppure fisica (ad es., rottura dei supporti di memorizzazione) non autorizzata, accompagnata dall'impossibilità di ripristinare i dati, quale che sia la modalità applicabile (ad es., uso di copie di backup, recupero da copie dei dati presenti in altri archivi, rielaborazione e rigenerazione a partire da altri dati rimasti disponibili). La distruzione riguarda l'ambito di *disponibilità* dei dati personali.
- ***Perdita/furto*** - Perdita del controllo del supporto fisico di memorizzazione (ad es., privazione, sottrazione, smarrimento dei dispositivi contenti i dati oppure dei documenti cartacei). La violazione non sussiste solo nelle situazioni in cui si possa escludere con ragionevole certezza l'acquisizione dei dati da parte di terzi - anche a priori non noti - e la perdita dei supporti non causi una "distruzione" dei dati. La perdita riguarda, nell'impossibilità di recuperare in altro modo i dati, l'ambito di *disponibilità* dei dati

personali e può riguardare l'ambito della *confidenzialità* se i dati contenuti nel supporto risultano intellegibili.

- ***Modifica/alterazione*** - Modifiche non autorizzate o improprie dei dati, non rilevate e corrette nell'ambito dei processi interni, anche in grado di determinare la comunicazione di informazioni erronee ad Enti e/o soggetti esterni alla **CASALP SPA** (ad es., Istituzioni) o al pubblico (ad es., Internet, Pannelli a messaggio variabile, comunicazioni massive). Corrispondono a modifiche improprie dei dati, non rilevate e corrette, effettuate al di fuori dei processi operativi di trattamento dei dati svolti dagli incaricati autorizzati, oppure ai casi di modifiche con finalità fraudolente eseguite dagli incaricati autorizzati all'accesso. La modifica riguarda l'ambito di *integrità* e l'ambito della *confidenzialità*.
- ***Rivelazione/copia*** - Messa a disposizione non autorizzata o impropria dei dati personali, non corrispondenti a informazioni pubbliche, verso terze parti (ad es., singole persone fisiche o persone giuridiche, gruppi di soggetti, pubblico), anche non identificabili. La violazione sussiste solo nelle situazioni in cui non si possa escludere con ragionevole certezza l'acquisizione dei dati da parte terzi, anche a priori non noti. La rivelazione o la copia riguardano l'ambito della *confidenzialità*.
- ***Accesso/lettura*** - Effettivo accesso ai dati trattati dall'azienda da parte di soggetti non aventi diritto. Corrispondono ad accessi ai dati (anche in sola visualizzazione) effettivamente avvenuti al di fuori dei processi operativi di trattamento dei dati previsti e autorizzati. L'accesso non autorizzato riguarda l'ambito della *confidenzialità*.

6.9 REPORTISTICA PERIODICA PER IL CDA

Il TRV, **nella versione allargata a tutti i componenti** necessari per le diverse tipologie di evento, si riunisce almeno **ANNUALMENTE** per verificare l'idoneità delle misure di sicurezza adottate e quelle eventualmente da implementare.
Il Referente Interno Privacy coadiuvato dal DPO rende disponibile una reportistica sugli eventi segnalati nel periodo e su quelli classificati come violazione, riportando in particolare:

- Un'analisi di confronto con il trend degli anni precedenti;
- Un'analisi delle possibili cause comuni che hanno portato alle violazioni occorse;
- Un'analisi su possibili misure di sicurezza aggiuntive da implementare nel sistema di controllo della Società al fine di prevenire o mitigare altre possibili violazioni.

6.10 MONITORAGGIO DELLA SICUREZZA

Il Dirigente /Responsabile dei Sistemi Informativi e l'Amministratore di sistema, per i propri ambiti di competenza, adottano e programmano processi (preventivi e proattivi) di **misurazione, monitoraggio e rendicontazione del livello di efficacia delle misure di sicurezza previste.**

6.10.1 MONITORAGGIO DELLA SICUREZZA ICT

A titolo esemplificativo e non esaustivo, di seguito sono proposti **alcuni processi di misurazione, monitoraggio e rendicontazione del livello di efficacia delle misure di sicurezza previste in ambito ICT**:

- ***Identificazione delle vulnerabilità dei sistemi ICT*** che trattano dati personali. Tale attività prevede la conduzione di Vulnerability Assessment. Tale attività produce una reportistica contenente le vulnerabilità identificate, i sistemi ICT coinvolti, il livello di criticità delle vulnerabilità in oggetto e le azioni di mitigazione proposte;
- ***Gestione del patching dei sistemi* ICT** che trattano dati personali. Il processo continuativo di patching assicura che le patch di sicurezza siano applicate con tempistiche legate al livello di criticità delle vulnerabilità sottese e minimizzando il rischio di disservizi dei sistemi ICT. Il monitoraggio di tale attività produce una reportistica relativa alle operazioni di applicazione delle patch per i sistemi ICT che trattano dati personale;
- ***Gestione delle configurazioni dei sistemi di sicurezza*.** Tale processo prevede il mantenimento e l'aggiornamento continuo delle configurazioni dei sistemi di sicurezza (ad es., signature antivirus). Tale attività produce una reportistica contenente il livello di conformità rispetto a politiche di configurazione e aggiornamento.

Tali attività, compiute anche tramite il supporto di soggetti esterni, potranno essere oggetto di report e rendiconti da condividere durante le riunioni periodiche di cui al punto 6.8.

6.10.2 MONITORAGGIO DELLA SICUREZZA FISICA

A titolo esemplificativo e non esaustivo, di seguito sono proposti alcuni processi di misurazione, monitoraggio e rendicontazione del livello di efficacia delle misure di sicurezza previste in ambito sicurezza fisica:

- ***Gestione dei presidi di sicurezza fisica*.** Tale processo prevede l'identificazione delle non conformità rispetto alle politiche e ai requisiti di sicurezza dei locali e degli archivi che contengono asset fisici che contengono dati personali (ad es.. Accesso alle sedi, CED, archivi centrali cartacei, uffici del Personale in cui sono presenti armadi contenenti le cartelle dei dipendenti, etc.);
- ***Gestione sistemi antincendio e misure di prevenzioni contro gli eventi distruttivi.*** Tale processo prevede l'implementazione di misure proattive nel confronto di eventi distruttivi quali incendi, allagamenti, terremoti o altro.

7. ALTRA DOCUMENTAZIONE

Fanno parte della presente procedura i seguenti moduli:

- "Inventario Elenco delle violazioni";
- "Modello segnalazione Data Breach".