PROCEDURA PRIVACY

Procedura per la gestione delle violazioni di dati personali

Rev.	Data	Oggetto	Responsabilità
/	29/06/2022	Aggiornamento del documento	**Elaborato da**: Avvera S.r.l.
			Verificato da: CIN S.p.A
			Approvato da: CIN S.p.A

INDICE

1. PREMESSA

La politica di sicurezza adottata dalla Società prevede che siano messe in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al General Data Protection Regulation (Regolamento UE 2016/679).

Ove però, nonostante tali interventi, si verifichi una violazione dei dati personali, la Società deve attivarsi prontamente per reagire a tale violazione, al fine di garantire il rispetto degli obiettivi di sicurezza:

- **Disponibilità**: ovvero, garantire l'accesso alle informazioni e ai servizi di rete da parte del personale incaricato in relazione alle esigenze lavorative, ai diritti e alle libertà fondamentali degli interessati;
- **Riservatezza**: ovvero, garantire la prevenzione di accessi abusivi o non autorizzati alle informazioni, ai servizi e ai sistemi;
- **Integrità**: ovvero, garantire che le informazioni non siano state alterate da incidenti o abusi;
- **Resilienza**: ovvero la capacità di un sistema di adattarsi ai cambiamenti.

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche quali ad esempio: discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, danno economico o sociale significativo, danno alla vita coniugale o di relazione, ecc.

La presente procedura delinea pertanto le responsabilità e le modalità di gestione della violazione dei dati personali per assicurarne una corretta gestione.

2. AMBITO DI APPLICAZIONE

I principi disciplinati dal presente documento si applicano al trattamento di dati personali ogni qualvolta si verifica una violazione dei dati stessi.

3. RESPONSABILITÀ DI ATTUAZIONE

Responsabile dell'attuazione della presente procedura, di concerto con il Titolare del trattamento e del Responsabile della Protezione dei Dati sono i coordinatori privacy eventualmente nominati.

4. DISTRIBUZIONE

La presente procedura ha come destinatari tutto il personale di CIN S.p.A.

5. DEFINIZIONI

Termine	Definizione
Coordinatore privacy	La persona fisica che, all'interno della struttura gerarchica del Titolare del trattamento, è preposta da quest'ultimo a concorrere alla determinazione delle modalità e finalità del trattamento
Danneggiamento	Evento che colpisce il dato personale e ha come conseguenza che il dato stesso è stato modificato, danneggiato o comunque non è più integro.
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.
Disponibilità	Caratteristica del dato personale che indica l'accessibilità dello stesso a chi ne ha diritto e nel momento in cui servono.
Distruzione	Evento che colpisce il dato personale e ha come conseguenza che il dato stesso non esiste più o non esiste in una forma utilizzabile dal titolare del trattamento.
DPO/RPD	Data Protection Officer / Responsabile della Protezione dei Dati.
GDPR/RGPD	General Data Protection Regulation (Regolamento UE 2016/679) / Regolamento generale sulla protezione dei dati (Regolamento UE 2016/679)
Integrità	Caratteristica del dato personale che ricomprende elementi di correttezza, coerenza, affidabilità e completezza.
Interessato	La persona fisica a cui si riferiscono i dati personali.
Perdita	Evento che colpisce il dato personale e ha come conseguenza che il titolare ne ha perso il controllo, l'accesso o la proprietà.
Persona autorizzata al trattamento	Chiunque agisca sotto l'autorità del titolare del trattamento o del Coordinatore privacy, che abbia accesso a dati personali e che sia istruito in tal senso.
Resilienza	La resilianza è la capacità di un sistema di adattarsi ai cambiamenti
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Riservatezza	Caratteristica del dato personale che non deve essere disponibile o divulgata a terzi.
Terzo	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Termine	Definizione
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Trattamento non autorizzato o non conforme alla legge	Evento che colpisce il dato personale e ha come conseguenza che esso diviene visibile a terzi o che terzi vi effettuano trattamenti in assenza di un titolo autorizzativo.
Violazione dei dati personali	La violazione di sicurezza (breach of security) che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati
Violazione della disponibilità	La violazione della disponibilità consiste in una perdita di accesso o distruzione di dati personali non autorizzata o casuale.
Violazione della integrità	La violazione della integrità consiste in una modifica di dati personali non autorizzata o casuale.
Violazione della riservatezza	La violazione della riservatezza consiste in una visibilità o un accesso a dati personali non autorizzata o casuale.

6. PRINCIPI GENERALI PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Il Regolamento UE 2016/679 (GDPR) definisce "*violazione dei dati personali*" la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati. Tale violazione incide sulla perdita di riservatezza, sul danneggiamento e sulla indisponibilità dei dati.

La Società ha, quindi, predisposto un sistema di gestione della violazione dei dati personali che è in grado, una volta rilevati gli incidenti, di rispondere adeguatamente ad essi, recuperare i dati compromessi tempestivamente ed efficacemente.

In particolare sono stati distinti tre differenti tipologie di violazioni che possono essere anche combinate reciprocamente:

1. **violazione di riservatezza**, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.
2. **violazione di integrità**, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
3. **violazione di disponibilità**, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

6.1 RILEVAZIONE E VALUTAZIONE DI UNA VIOLAZIONE DI SICUREZZA

Il Titolare del trattamento e i coordinatori privacy devono gestire la violazione di dati personali e gli obblighi di notifica e informativa, coordinando tra loro le attività da compiere e informando immediatamente il Responsabile della Protezione dei Dati (DPO). A seguito di una violazione di dati personali il Titolare e il DPO, con l'ausilio dei coordinatori privacy, devono:

1	Identificare se la violazione di sicurezza consista in violazione su dati personali, ovvero, stabiliscono se essa abbia ad oggetto dati personali
2	Valutare se la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche
3	Qualora a seguito di tale preliminare analisi emerga un impatto sui diritti e sulle libertà delle persone fisiche, effettuare una successiva valutazione del livello di rischio[1] utilizzando i seguenti parametri (*Rif. WP 29*): • Tipo di violazione • Natura, sensibilità e volume dei dati personali • Facilità di riconoscimento degli interessati • Serietà delle conseguenze per le persone fisiche • Caratteristiche specifiche delle persone fisiche • Quantità di persone fisiche coinvolte • Caratteristiche specifiche del titolare
4	Curare la notifica (o una prima notifica) all'autorità di controllo entro 72 ore dalla apprensione della violazione di sicurezza
5	Integrare – se necessario – la prima notifica o ritirarla in ragione di approfondimenti svolti
6	Avviare e guidare il processo di comunicazione all'interessato (ove valutato necessario / opportuno)
7	Programmare e attuare un piano di azione per implementare le azioni correttive per prevenire future analoghe violazioni e mitigarne le conseguenze

[1] *La valutazione del rischio viene effettuata in termini di impatto rispetto ai dati personali ed ai diritti e la libertà degli interessati.*

8	Curare la tenuta di idonea documentazione per dimostrare la gestione della violazione di sicurezza (indipendentemente dallo svolgimento di tutte le successive fasi).

Tabella 1

Se - a seguito di tale valutazione - l'evento risulta non avere impatto sui diritti e sulle libertà fondamentali dell'interessato, questo verrà documentato e archiviato. Tutte le attività conseguenti ad un evento che impatta sulla sicurezza dei dati personali devono essere tracciate con possibilità di replicazione anche al fine di fornire evidenza nelle sedi competenti. In caso di dubbio, sull'esposizione e sul livello di rischio, il DPO deve procedere sempre alla notificazione al Garante.

Chiunque venga a conoscenza, anche attraverso canali non ufficiali, di un incidente di sicurezza ha l'obbligo perentorio di darne immediata comunicazione, tracciabile (ad es. con email), al Titolare del trattamento e al coordinatore privacy eventualmente nominato. In allegato alla presente procedura si riporta una sintetica istruzione in merito alla segnalazione di possibili violazioni della sicurezza o di elementi indicatori di tali violazioni (*Rif. Allegato 1*).

Parallelamente alle attività di cui alla Tabella 1 il Titolare del trattamento e i coordinatori privacy si devono coordinare sulle attività da porre in essere volte a:

1	Garantire l'immediata cessazione della violazione dei dati personali (qualora risulti ancora in essere), prendendo tutte le precauzioni necessarie per evitare ulteriori perdite di dati, bloccando l'accesso non autorizzato ai sistemi/dati e conservando gli elementi di prova per successive investigazioni ed analisi
2	Individuare la portata e le dimensioni dei dati personali coinvolti dalla violazione
3	Analizzare l'efficacia delle misure tecniche ed organizzative mitigative implementate
4	Valutare gli eventi relativi alla sicurezza delle informazioni e decidere se classificarli come incidenti o meno

Tabella 2

I Responsabili del trattamento esterni a cui sono affidati i servizi sono vincolati mediante clausole contrattuali che regolano il rapporto di fornitura a segnalare tempestivamente e adeguatamente una violazione di sicurezza, senza ritardo ed in modo esaustivo (*Rif. art. 33 GDPR*). Ciò premesso, al verificarsi di un incidente di sicurezza sulle strutture, logiche e fisiche, del Responsabile del trattamento, quest'ultimo deve informare, immediatamente, il Titolare del trattamento e il DPO per renderli edotti dell'accaduto. Il Titolare del trattamento e i coordinatori privacy devono prendere tutte le decisioni in merito per monitorare e vigilare sull'impatto di tale evento sui dati personali trattati dalla Società .

6.1.1 VIOLAZIONE DEI DATI PERSONALI: NOTIFICA AL GARANTE

Una volta accertata una violazione dei dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche il nominato DPO deve:

1. procedere alla tempestiva notificazione all'autorità di controllo **entro le 72 ore**,
2. in caso di ritardo nella notificazione, addurre giustificazioni,
3. iscrivere l'accadimento nell'apposito Registro sulle Violazioni (*Rif. paragrafo 6.2*),
4. istruire il personale che è a conoscenza della violazione di mantenere i dettagli di violazione riservati fino a diversa comunicazione ufficiale,
5. documentare quanto messo in atto per ridurre i potenziali rischi;
6. definire ed applicare opportune procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione di informazioni relative agli incidenti di sicurezza che possano essere impiegate come evidenze.

La normativa di riferimento indica il contenuto minimo della notificazione al Garante nei seguenti elementi:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati (DPO/RPD) o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o 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.

Il Titolare del trattamento deve quindi procedere con la notificazione all'autorità Garante fornendo le informazioni indicate nell'allegato al Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali riportati al seguente link: https://www.garanteprivacy.it/documents/10160/0/Modello+notifica+Data+Breach.pdf/6d1fa433-88dc-2711-22ab-dd5d476abe74?version=1.2.

La notifica deve essere inviata all'Autorità Garante tramite posta elettronica all'indirizzo protocollo@pec.gpdp.it mediante casella di posta certificata (l'indirizzo è configurato per ricevere solo comunicazioni provenienti da posta elettronica certificata) o mediante posta elettronica ordinaria all'indirizzo protocollo@gpdp.it e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

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

Qualora e nella misura in cui non sia possibile proporre le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo. Tuttavia, qualora sussistano più violazioni che incidono con la stessa modalità la confidenzialità dei dati trattati in un breve lasso di tempo, la Società dovrà effettuare un'unica notificazione all'Autorità Garante ponendo, come giustificazione per il ritardo, tale onerosità e omogeneità di violazione.

6.1.2 GESTIONE DELLE RISPOSTE AD UNA VIOLAZIONE DI DATI PERSONALI – "NOTIFICA PER FASI"

Qualora la Società sia vittima di violazioni complesse che involgono, ad esempio, cyber attacchi alla sicurezza e per i quali sia, comunque, necessario condurre indagini approfondite, i risultati di tali approfondimenti dovranno essere notificati al Garante in differenti fasi susseguenti e senza giustificato ritardo.

In tali casi il Titolare del trattamento dovrà effettuare le indagini avvalendosi dei coordinatori privacy e comunicare al Garante, in sede di prima notificazione, l'informazione che trattasi di violazione complessa che richiede un approfondimento di indagine e ulteriori informazioni verranno inviate progressivamente allo sviluppo delle indagini.

Se, a seguito del grado di maturità raggiunto nelle indagini, risulta che l'evento verificatosi ha avuto un effetto contenuto e che nessuna violazione si è perpetrata, dovrà essere data evidenza al Garante con apposita notificazione successiva.

6.1.3 GESTIONE DELLE RISPOSTE AD UNA VIOLAZIONE DI DATI PERSONALI – COMUNICAZIONE ALL'INTERESSATO

Il Titolare del trattamento deve comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie (*Rif. art. 34 del GDPR*).

La Comunicazione all'interessato non va eseguita qualora:

a) siano 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 o la pseudonimizzazione;
b) siano adottate misure mitigative atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.

La comunicazione all'interessato deve descrivere la natura della violazione dei dati personali e deve contenere raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge[2].

La comunicazione all'interessato deve essere eseguita dal Titolare del trattamento, anche con il supporto del DPO, inviando direttamente e personalmente all'interessato una email o altra comunicazione a lui direttamente destinata e che consenta di tracciare la lettura da parte dell'interessato descrivendo, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali e con, almeno, le informazioni e le misure seguenti:

a) il nome e i dati di contatto del responsabile della protezione dei dati (DPO / RPD) o di altro punto di contatto presso cui ottenere più informazioni;
b) le probabili conseguenze della violazione dei dati personali;

[2] *La necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione.*

c) 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.

La comunicazione deve essere chiara, inequivocabile e richiamare l'attenzione dell'interessato. Non deve essere confusa con altre comunicazioni o contenuti che usualmente sono inviati all'interessato (es. reportistica, newsletter, promozioni, etc). Nei casi in cui il numero degli interessati coinvolti o la loro indeterminatezza rende una comunicazione pubblica generalizzata essa può essere resa mediante banner del website della Società (con traduzione in inglese), comunicazioni massive o altri metodi idonei a raggiungere con successo tutti gli interessati coinvolti.

6.2 REGISTRO SULLE VIOLAZIONI

A cura del DPO, con il supporto dei coordinatori privacy, è la tenuta del "**Registro sulle Violazioni**" ove vengono annotati tutti i riferimenti circa gli eventi sia quelli che hanno avuto impatto su dati personali, sia quelli che – dopo valutazione – non sono stati considerati tali. Il Registro ha lo scopo di:

- individuare e analizzare i fattori di rischio,
- identificare la natura della violazione più frequente,
- misurare l'efficacia delle procedure adottate,
- elaborare un Piano di Conformità che determini gli obiettivi di compliance, nonché le best practices e che sia di supporto ai fini di dimostrare la conformità in sede di verifica di Audit e di Ispezioni dell'Autorità di controllo e delle Autorità ispettive.

Per ogni evento devono essere indicate nel registro le seguenti informazioni:

- i dettagli concernenti l'evento,
- le possibili cause individuate,
- le misure adottate,
- il riferimento alla documentazione delle misure implementate per affrontare la violazione con annesse le relative motivazioni di scelta,
- le valutazioni dell'Autorità di controllo, ove sia stata coinvolta.

ALLEGATO 1

Tutte le persone autorizzate della Società possono rilevare una violazione dei dati personali. In particolare i soggetti che ricoprono il ruolo di Amministratore di Sistema e in generale tutti gli utilizzatori di sistema informatico sono tenuti a segnalare con tempestività ogni anomalia che possa essere indicativa di una violazione.

Per stabilire se un determinato evento/comportamento sia indicativo di una violazione, bisogna considerare eventi quali, a titolo esemplificativo e non esaustivo:

- le problematiche connesse all'uso degli account personali;
- la visibilità di dati e/o sistemi non di propria competenza;
- la modifica e/o la sparizione di dati;
- smarrimento di asset aziendali;
- infrazioni della proprietà aziendale.

L'evento – o il comportamento – indicativo di una violazione deve immediatamente essere segnalato al DPO e al coordinatore privacy competente.