

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (Data Breach)



 SOSTELIA Società del Gruppo Hera	Procedura per la gestione delle violazioni di dati personali (data breach)	Rev. 03 del 09/06/2026
	Modello Organizzativo Privacy	

Tabella di revisione:

Controllo del documento	
Autore	Lucrezia Lodi
Data di creazione	05/06/2023
Autore della revisione	Lucrezia Lodi
Data di ultima revisione	09/06/2026

Versione	Data	Approvato da	Descrizione delle modifiche
00	05/06/2023	Direzione	Prima emissione
01	27/06/2025	Direzione	Seconda emissione
02	04/09/2025	Direzione	Terza emissione
03	09/06/2026	Direzione	Adeguamento a Sostelia S.p.A. A Socio Unico

La riproduzione del presente documento è vietata senza la preventiva autorizzazione

SOMMARIO:

PREMESSA 4

SCOPO E AMBITO DI APPLICAZIONE..... 4

RIFERIMENTI NORMATIVI 4

DEFINIZIONI 4

GESTIONE DEL DATA BREACH..... 5

GESTIONE DEI DATA BREACH ESTERNI 6

COMUNICAZIONE AGLI INTERESSATI 6

SCHEMA VALUTAZIONE SCENARI DI DATA BREACH 7

REGISTRO DELLE VIOLAZIONI 8

REFERENTI PER LA GESTIONE DEI DATA BREACH 8

COMUNICAZIONI 8

ENTRATA IN VIGORE 8

PREMESSA

Una violazione dei dati personali (data breach) può, se non affrontata tempestivamente e correttamente, causare danni fisici, materiali o immateriali agli interessati. Tali danni possono consistere, ad esempio, nella perdita del controllo sui propri dati personali, nella discriminazione, furto o usurpazione d'identità, danni reputazionali o economici.

Nel contesto delle attività svolte dalla Società, il trattamento dei dati personali riveste un'importanza cruciale in quanto coinvolge quotidianamente informazioni sensibili relative a utenti dei servizi, personale, collaboratori e fornitori. Pertanto, la gestione corretta e tempestiva di eventuali violazioni rappresenta non solo un obbligo giuridico ai sensi del Regolamento UE 2016/679 (GDPR), ma anche un dovere etico verso le persone di cui si trattano i dati.

Il data breach, infatti, può derivare non solo da attacchi informatici o azioni dolose, ma anche da errori umani, smarrimenti di dispositivi, incidenti fisici o malfunzionamenti tecnici. In tutti questi casi, una pronta rilevazione e una risposta organizzata ed efficace sono essenziali per minimizzare le conseguenze negative e per adempiere agli obblighi normativi, inclusa la comunicazione tempestiva alle Autorità e, se necessario, agli interessati.

La presente procedura vuole promuovere una cultura della prevenzione e della sicurezza, garantendo che tutto il personale sia sensibilizzato e formato sul corretto comportamento da adottare in caso di incidente, nonché sulla necessità di agire in stretta collaborazione con il Referente Privacy e il DPO per la gestione degli eventi e il rispetto delle tempistiche previste dalla normativa.

SCOPO E AMBITO DI APPLICAZIONE

La presente procedura si applica a **Sostelia S.p.A. A Socio Unico**

Essa si prefigge lo scopo di definire le modalità di gestione dei data breach in conformità al Regolamento UE 2016/679 (GDPR), al D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018, alle Linee Guida del Garante per la protezione dei dati personali.

La procedura si applica a tutti i trattamenti di dati personali effettuati all'interno delle strutture gestite dall'Organizzazione, sia in formato digitale che cartaceo, e coinvolge tutto il personale dipendente, collaboratori, consulenti esterni e fornitori nominati Responsabili del trattamento, in quanto potenzialmente coinvolti nella gestione o nella segnalazione di eventi di violazione dei dati.

L'obiettivo è garantire un approccio tempestivo, sistematico e conforme alla normativa per l'identificazione, la gestione, la comunicazione e la risoluzione delle violazioni dei dati personali, tutelando così i diritti e le libertà degli interessati e minimizzando i potenziali impatti negativi per l'Organizzazione e per le persone coinvolte.

RIFERIMENTI NORMATIVI

- Regolamento UE 2016/679 (GDPR), in particolare gli articoli 33 e 34 relativi alla notifica delle violazioni dei dati personali.
- Decreto Legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) come modificato dal D.Lgs. 10 agosto 2018, n. 101.
- Linee Guida EDPB 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del GDPR – Versione 2.0, adottate il 28 marzo 2023 (aggiornamento delle linee guida WP250 rev.01 del Gruppo di lavoro Articolo 29, approvate dall'EDPB nella prima riunione plenaria del 25 maggio 2018).
- Considerando 85, 86, 87 e 88 del GDPR relativi ai rischi per i diritti e le libertà delle persone fisiche in caso di violazione.
- Provvedimenti e comunicazioni ufficiali dell'Autorità Garante per la Protezione dei Dati Personali.
- Linee Guida e toolkit operativi per la gestione dei Data Breach disponibili sul sito istituzionale del Garante (www.garanteprivacy.it).

DEFINIZIONI

 SOSTELIA Società del Gruppo Hera	Procedura per la gestione delle violazioni di dati personali (data breach) Modello Organizzativo Privacy	Rev. 03 del 09/06/2026
--	--	---------------------------

Le definizioni principali utilizzate nella presente procedura sono conformi all'art. 4 del Regolamento UE 2016/679 (GDPR):

- **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, mediante 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.
- **Trattamento:** qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la modifica, l'estrazione, la consultazione, l'uso, la comunicazione, la diffusione, la cancellazione o la distruzione.
- **Archivio:** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dalla sua forma (digitale o cartacea).
- **Titolare del trattamento:** la persona fisica o giuridica, autorità pubblica, servizio o altro organismo che determina le finalità e i mezzi del trattamento di dati personali.
- **Referente Privacy:** la figura interna designata per supportare il Titolare nella gestione operativa delle attività privacy e nella valutazione e gestione di eventuali violazioni.
- **Data Protection Officer (DPO):** la persona fisica o giuridica designata ai sensi degli artt. 37-39 del GDPR per sorvegliare l'osservanza della normativa e fungere da punto di contatto con l'Autorità Garante.
- **Autorizzato al trattamento:** la persona fisica autorizzata dal Titolare o dal Responsabile del trattamento a trattare dati personali sotto la loro diretta autorità.
- **Responsabile del trattamento:** la persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del Titolare.
- **Violazione dei dati personali (Data Breach):** una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
- **Interessato:** la persona fisica cui si riferiscono i dati personali oggetto di trattamento.
- **Misure tecniche e organizzative:** gli strumenti e le procedure messe in atto dal Titolare per garantire un livello di sicurezza adeguato al rischio.
- **Rischio per i diritti e le libertà:** la possibilità che una violazione dei dati personali possa determinare conseguenze negative per l'interessato, come la discriminazione, l'usurpazione di identità, la perdita di riservatezza o danni economici.

Queste definizioni costituiscono la base terminologica per la corretta comprensione e applicazione della presente procedura.

GESTIONE DEL DATA BREACH

Ogni operatore che venga a conoscenza di un potenziale data breach deve informare tempestivamente il Referente Privacy aziendale. Quest'ultimo, con il supporto del DPO (se nominato) e dell'Amministratore di Sistema, valuta l'accaduto utilizzando lo schema di scenario allegato e l'autovalutazione del Garante.

Per effettuare la valutazione preliminare del data breach, il Referente Privacy potrà avvalersi del tool di autovalutazione messo a disposizione dall'Autorità Garante per la Protezione dei Dati Personali, disponibile al seguente link: <https://servizi.gpdp.it/databreach/s/self-assessment>

In caso di conferma, la notifica all'Autorità Garante verrà predisposta dal Referente Privacy, a firma del Titolare, entro 72 ore dall'avvenuta conoscenza dell'incidente. L'invio della notifica deve essere effettuato tramite il modulo online disponibile al seguente link: <https://servizi.gpdp.it/databreach/s/scelta-auth>

Ai fini della presente procedura, il Titolare del trattamento si considera "venuto a conoscenza" di una violazione nel momento in cui ha un ragionevole grado di certezza che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali (EDPB Guidelines 9/2022, § II.B). Il periodo

di indagine preliminare, nel corso del quale si verifica se l'incidente costituisca effettivamente un data breach, non fa decorrere il termine delle 72 ore.

La notifica al Garante non è dovuta qualora sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche (art. 33, par. 1, GDPR). Un esempio tipico: la perdita di un dispositivo mobile correttamente cifrato con chiave intatta e con backup disponibile. In caso di dubbio, il Titolare deve propendere per la notifica.

Eventuali ritardi devono essere motivati e documentati.

Il processo di gestione del data breach include:

- Segnalazione interna immediata da parte del personale;
- Contenimento immediato dell'incidente: isolamento dei sistemi coinvolti, revoca degli accessi non autorizzati, blocco di eventuali trasmissioni in corso e preservazione dei log ai fini dell'analisi forense;
- Valutazione tecnica e giuridica dell'evento;
- Classificazione del rischio e decisione sulla necessità di notifica;
- Notifica per fasi all'Autorità Garante: qualora non siano disponibili tutte le informazioni entro 72 ore, è consentito effettuare una prima notifica con i dati disponibili e integrare successivamente, senza ulteriore ingiustificato ritardo (art. 33, par. 4, GDPR);
- Eventuale comunicazione agli interessati se il rischio risulta elevato;
- Registrazione dettagliata dell'evento nel Registro delle violazioni.

Tutti i passaggi devono essere gestiti con tempestività, trasparenza e conformità alle disposizioni normative per garantire la tutela degli interessati e la minimizzazione dei rischi per L'Organizzazione.

GESTIONE DEI DATA BREACH ESTERNI

In caso di affidamento di trattamenti di dati personali a soggetti terzi, la presente procedura deve essere recepita e formalizzata nei contratti di nomina a Responsabile esterno del trattamento, come previsto dall'art. 28 del GDPR. Tali contratti devono includere clausole specifiche volte a garantire che il Responsabile del trattamento adotti misure tecniche e organizzative adeguate per prevenire violazioni dei dati e per garantire il rispetto dei principi di integrità, riservatezza e disponibilità delle informazioni.

Eventuali violazioni dei dati personali commesse da parte di tali Responsabili esterni devono essere comunicate senza ingiustificato ritardo al Referente Privacy dell'Organizzazione, il quale provvederà alla valutazione del rischio e, se necessario, alla predisposizione delle comunicazioni obbligatorie nei confronti dell'Autorità Garante e degli interessati.

Il Responsabile esterno è inoltre tenuto a garantire che i propri dipendenti, collaboratori e sub-fornitori siano adeguatamente formati e sensibilizzati sui temi della sicurezza dei dati e del data breach, adottando procedure interne coerenti con la normativa vigente e con le indicazioni fornite dal Titolare del trattamento. Particolare attenzione deve essere prestata nei casi in cui i Responsabili esterni trattino dati particolari o dati relativi a categorie vulnerabili di interessati (es. dati sanitari, dati di minori o di soggetti fragili), in quanto il potenziale impatto di una violazione potrebbe comportare conseguenze significative per i diritti e le libertà fondamentali degli interessati.

Nel caso di utilizzo di servizi cloud, piattaforme tecnologiche o strumenti digitali forniti da terze parti, è responsabilità del Titolare del trattamento verificare preventivamente l'adeguatezza dei fornitori in termini di sicurezza e protezione dei dati, anche attraverso la stipula di accordi specifici e la previsione di audit periodici. I fornitori dovranno altresì garantire il rispetto delle tempistiche e delle modalità di notifica in caso di eventuale data breach.

COMUNICAZIONE AGLI INTERESSATI

Qualora la violazione possa comportare un rischio elevato per i diritti e le libertà degli interessati, questi devono essere informati senza ingiustificato ritardo, in conformità all'art. 34 del GDPR.

La comunicazione sarà predisposta dal Referente Privacy e a firma del Titolare, e dovrà:

- Essere redatta in modo chiaro, semplice e facilmente comprensibile, evitando tecnicismi eccessivi.
- Descrivere in maniera concisa e trasparente la natura della violazione dei dati personali.
- Indicare il nome e i dati di contatto del DPO (se nominato) o di altro punto di contatto presso cui ottenere ulteriori informazioni.
- Fornire una descrizione delle probabili conseguenze della violazione dei dati personali.
- Indicare le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e, se del caso, le misure per attenuarne i possibili effetti negativi.
- Raccomandare agli interessati eventuali azioni pratiche da intraprendere per proteggersi (es. modifica delle password, attenzione a comunicazioni sospette, monitoraggio dei movimenti bancari, ecc.).

La comunicazione agli interessati non è dovuta, ai sensi dell'art. 34, par. 3, GDPR, se ricorre almeno una delle seguenti condizioni: (a) il Titolare ha adottato misure tecniche adeguate che rendono i dati incomprensibili ai soggetti non autorizzati, in particolare mediante cifratura allo stato dell'arte o tokenizzazione; (b) il Titolare ha adottato, immediatamente dopo la violazione, misure tali da garantire che non si concretizzi più il rischio elevato per i diritti e le libertà degli interessati; (c) la comunicazione diretta richiederebbe uno sforzo sproporzionato: in tale caso l'Organizzazione ricorrerà a una comunicazione pubblica o misura equivalente altrettanto efficace. Qualora il Titolare decida di non procedere alla comunicazione, l'Autorità Garante può comunque ordinare che essa venga effettuata, ove ritenga che la violazione presenti un rischio elevato per gli interessati (art. 34, par. 4, GDPR).

Tutte le comunicazioni dovranno essere documentate e conservate, con la relativa prova di invio o pubblicazione, ai fini di eventuali controlli da parte dell'Autorità Garante e per garantire la massima trasparenza e accountability dell'organizzazione.

SCHEMA VALUTAZIONE SCENARI DI DATA BREACH

La procedura include esempi, soglie e criteri di valutazione per supportare il Referente Privacy, il DPO e i soggetti coinvolti nella corretta classificazione degli incidenti e nella decisione in merito alla necessità di notifica all'Autorità Garante o di comunicazione agli interessati. I principali scenari considerati sono i seguenti:

- **Distruzione:** perdita definitiva e irreversibile dei dati, non più disponibili né per il Titolare né per l'interessato. Rilevante se i dati erano unici e definitivi.
- **Perdita:** dati non più nella disponibilità del Titolare ma potenzialmente accessibili a terzi, con rischio di divulgazione impropria.
- **Divulgazione non autorizzata:** diffusione dei dati a soggetti non autorizzati o pubblicazione non intenzionale.
- **Accesso non autorizzato:** dati visualizzati o utilizzati da soggetti non autorizzati, anche interni, senza necessità di divulgazione esterna.
- **Indisponibilità temporanea:** interruzione prolungata di accesso ai dati, tale da compromettere la capacità di erogazione dei servizi o i diritti degli interessati.
- **Modifica irreversibile:** alterazione dei dati senza possibilità di ripristino del loro valore originario o attendibilità.

Per ogni scenario, la valutazione dovrà considerare:

- La natura dei dati coinvolti (es. dati particolari, sanitari, giudiziari);
- Il volume dei dati e il numero di interessati;
- Il contesto e la natura dell'incidente;
- Il potenziale impatto per gli interessati (es. danni materiali, reputazionali, violazioni di diritti fondamentali);
- Le misure già presenti o adottabili per limitare il rischio.

La valutazione potrà essere supportata dall'utilizzo dello strumento di autovalutazione del Garante (<https://servizi.gpdp.it/databreach/s/self-assessment>) e dovrà essere documentata nel fascicolo del singolo incidente.

L'approccio basato sul rischio e sulla gradualità consente di distinguere tra eventi che richiedono la sola registrazione interna e quelli che impongono la notifica formale o la comunicazione agli interessati.

REGISTRO DELLE VIOLAZIONI

Il Referente Privacy mantiene e aggiorna il registro delle violazioni dei dati personali ai sensi dell'art. 33 del GDPR. Tale registro rappresenta uno strumento fondamentale per garantire la tracciabilità e la documentazione di tutte le violazioni, indipendentemente dalla loro gravità e dalla necessità o meno di notifica all'Autorità Garante.

Il registro deve contenere almeno le seguenti informazioni:

- Data e ora dell'incidente;
- Descrizione sintetica dell'accaduto;
- Categorie e volume dei dati coinvolti;
- Numero stimato di interessati;
- Azioni correttive adottate;
- Esito della valutazione del rischio;
- Eventuale notifica al Garante e/o comunicazione agli interessati;
- Data di chiusura dell'evento.

Il registro deve essere conservato in modo sicuro e accessibile solo al personale autorizzato, e potrà essere esibito in caso di richiesta da parte dell'Autorità di controllo.

L'obbligo di documentazione si applica a tutte le violazioni, comprese quelle per le quali si è deciso di non procedere alla notifica al Garante: in tali casi il registro deve riportare le motivazioni della mancata notifica, a dimostrazione del rispetto del principio di responsabilizzazione (accountability) di cui all'art. 5, par. 2, GDPR e dell'art. 33, par. 5, GDPR.

REFERENTI PER LA GESTIONE DEI DATA BREACH

Eventuali violazioni di dati personali sono da comunicare ai seguenti soggetti:

- Referente Privacy: Lucrezia Lodi – mail: lucrezia.lodi@sostelia.it
- Responsabile IT: Francesco Riccò – mail: informatica@sostelia.com

COMUNICAZIONI

La presente procedura è resa disponibile a tutto il personale dell'Organizzazione mediante pubblicazione sulle bacheche aziendali, invio tramite e-mail istituzionale e, ove presente, caricamento sull'intranet aziendale o su piattaforme di comunicazione interna.

A ogni aggiornamento del documento, il personale sarà informato tempestivamente attraverso i medesimi canali. È obbligo di ciascun dipendente e collaboratore prendere visione della versione più aggiornata e conformarsi integralmente alle disposizioni contenute.

La mancata osservanza delle disposizioni potrà comportare l'applicazione di sanzioni disciplinari, oltre all'eventuale segnalazione alle autorità competenti nei casi di violazioni gravi o reiterate.

ENTRATA IN VIGORE

La presente procedura entra in vigore a partire dal 09/06/2026 e sostituisce integralmente ogni precedente disposizione in materia di gestione dei data breach adottata dall'Organizzazione.

Il documento è soggetto a revisione periodica almeno annuale, o ogniqualvolta si verifichino cambiamenti significativi nelle normative di riferimento o nelle modalità operative.

L'eventuale aggiornamento sarà comunicato in modo formale a tutti i destinatari e la versione aggiornata sarà resa disponibile secondo le modalità indicate nella sezione "Comunicazioni".

SCHEMA DI VALUTAZIONE SCENARI DATA BREACH

Tipo di Breach	Definizione	Estensione Minima / Soglia di Segnalazione	Esempi	Controesempi (non necessita di segnalazione)
Distruzione	Perdita definitiva e irreversibile di dati personali, non più disponibili né per il Titolare né per l'interessato.	- Dati non recuperabili o provenienti da procedure non ripetibili.- Documenti definitivi con livello minimo di validazione.	- Guasto irreparabile dell'hard disk contenente referti salvati localmente.- Incendio di archivio cartaceo.	- Rottura di chiavetta USB senza dati originali unici.- Rottura di PC senza dati originali.- Distruzione di documento in fase di redazione.
Perdita	Dati non più nella disponibilità del Titolare, ma potenzialmente accessibili a terzi, con rischio di divulgazione impropria.	- Dati non recuperabili o provenienti da procedure non ripetibili.- Dati la cui perdita può ledere i diritti degli interessati.	- Smarrimento di chiavetta USB con dati originali.- Smarrimento fascicolo cartaceo personale.	- Smarrimento di documento in fase di stampa senza informazioni definitive.
Divulgazione non autorizzata	Trasmissione o diffusione impropria di dati personali a terzi non autorizzati.	- Dati appartenenti a documenti definitivi e validati.	- Invio errato di dati personali ad altra struttura.- Pubblicazione accidentale su web.	- Attacco hacker con furto ma senza diffusione.- Infezione di PC senza trasmissione dati.- Documento non ancora validato.
Accesso non autorizzato	Accesso ai dati personali da parte di soggetti non autorizzati.	- Accesso a dati definitivi e validati da parte di utenti non titolari.	- Accesso a rete aziendale da parte di esterni sfruttando vulnerabilità.- Accesso errato a dati non pertinenti.	- Accesso a dati di propria pertinenza ma uso improprio.- Accesso a documenti in bozza non validati.
Indisponibilità temporanea del dato	Interruzione temporanea di accesso ai dati che lede i diritti degli interessati.	- Indisponibilità superiore ai tempi definiti a livello aziendale.	- Ransomware che blocca i dati senza possibilità di ripristino immediato.- Perdita chiave crittografia.	- Manutenzione programmata di sistema.- Interruzione breve senza impatto su diritti degli interessati.
Modifica irreversibile	Alterazione permanente dei dati personali senza possibilità di ripristino certo.	- Modifiche sistematiche su più casi o dati definitivi.	- Guasto che altera contenuti di un sistema.- Modifica accidentale non tracciabile di dati.	- Guasto corretto tramite recovery.- Modifica tracciata e reversibile.- Documento non ancora validato.

Firmato digitalmente da:
Giuliano Fontanesi
Data: 10/06/2026 18:29:14