Procedura per la gestione del "Data Breach"

Sommario

ARGOMENTO	PAROLE CHIAVE	REQUISITI COLLEGATI
Violazione di sicurezza dei dati personali	Data Breach	

REDAZIONE	VERIFICA E CONTROLLO	APPROVAZIONE	CODICE DATA
Assistente Amministrativo Simoni Margherita	Servizio DPO-Upipa	Taufer Federica	06
			18.12.2025

DOCUMENTO PRECEDENTE	DATA EMISSIONE PRECEDENTE	CAUSALE DELLA REVISIONE
05	15.02.2023	Revisione: in caso di cambiamenti significativi e comunque massimo entro 3 anni dall'ultima revisione

Approvazione a cura di

NOME E COGNOME	RUOLO	STRUTTURA DI APPARTENENZA
Federica Taufer	Direttore	A.P.S.P "San Giuseppe" di Primiero

redazione a cura di (in ordine alfabetico):

Nome e Cognome	Ruolo	Struttura di appartenenza
Margherita Simoni	Assistente Amministrativo	A.P.S.P "San Giuseppe" di Primiero

Hanno collaborato (in ordine alfabetico):

Nome e Cognome	Ruolo	Struttura di appartenenza
Servizio DPO	Responsabile della Protezione dei Dati	Upipa

Verifica e controllo a cura di (in ordine alfabetico):

Nome e Cognome	Ruolo	Struttura di appartenenza
Servizio DPO	Responsabile della Protezione dei Dati	Upipa
Federica Taufer	Direttore	A.P.S.P "San Giuseppe"di Primiero

LISTA DELLE REVISIONI

REVISIONE N.	DATA	DESCRIZIONE DELLE MODIFICHE
00	28.05.2013	Prima emissione
01	09.05.2014	Aggiornamento contenuti

02	30.04.2019	Adeguamento al GDPR e al D.Lgs 101/18
03	12.12.2019	Inserimento allegato proc. data breach – revisione allegati (ambito e incarico unico doc.)
04	22.07.2022	Modifica punto 4) dell'istruzione del data breach Allegato nr. 4 "notifica della violazione al Garante"
05	15.02.2023	Modifica punto 4) dell'istruzione del data breach Allegato nr. 4 "notifica della violazione al Garante": aggiornamento link al sito istituzionale
06	18.12.2025	Adeguamento alla Procedura Gestione Data Breach rev. n. 2 Upipa Agosto 2022

1 – DEFINIZIONE DI DATA BREACH

Per "**Data Breach"** si intende un evento in conseguenza del quale si verifica una **"violazione dei dati personali"**. L'articolo 4 p.12 del GDPR definisce la "violazione dei dati personali" come 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**. L'art. 33 del GDPR prevede che **"in caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente** a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, **a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".

Le violazioni possono essere classificate in tre macro categorie che, a seconda dei casi, possono riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali (anche in combinazione):

1) "violazione della riservatezza" in caso **di divulgazione dei dati personali** o accesso agli stessi non autorizzati o accidentali;

2) "violazione dell'integrità del dato" in caso **di modifica non autorizzata** o **accidentale** dei dati personali;

3) "violazione della disponibilità del dato", in caso di **perdita**, **accesso** o **distruzione accidentali** o non autorizzati di dati personali.

A seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

A seconda delle circostanze in cui si verifica la violazione può richiedere o meno la notifica all'autorità di controllo e la comunicazione alle persone fisiche coinvolte.

Il titolare del trattamento, riscontrata una violazione, è tenuto di volta in volta a valutare la probabilità e la gravità del conseguente impatto sui diritti e sulle libertà delle persone fisiche e:

a) documentare la violazione nel proprio **Registro delle Violazioni** (sempre);

b) effettuare la **notifica al Garante** (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);

c) comunicare la **violazione ai soggetti interessati** (laddove possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte).

2 – SCOPO E CAMPO DI APPLICAZIONE

La presente procedura definisce le modalità di gestione del "data breach" che l'A.P.S.P. "San Giuseppe" di Primiero, titolare del trattamento, è tenuto ad osservare e far rispettare ai propri preposti.

3 – ELENCO DESTINATARI

La procedura è destinata a:

- Direzione dell'A.P.S.P. "San Giuseppe" di Primiero;
- Il DPO opera in qualità di soggetto informato e supervisore, non responsabile operativo della gestione del data breach
- Personale dipendente e collaboratori dell'Ente;
- Responsabili del trattamento esterni, per la parte di competenza;
- Stagisti, tirocinanti e personale convenzionato, se coinvolti nel trattamento di dati personali;
- Ogni ulteriore soggetto interno incaricato del trattamento dei dati personali.

Tutti i destinatari sono tenuti a conoscere e rispettare la presente procedura.

4 – MODALITÀ DI DISTRIBUZIONE

La presente procedura è resa disponibile affinché ogni destinatario possa prenderne piena conoscenza. In particolare:

- viene diffusa a tutto il personale dipendente mediante comunicazioni interne;
- è affissa nella bacheca interna dell'Ente;
- una copia cartacea è disponibile presso la Sala riunioni del personale ed è consultabile presso l'Ufficio Segreteria;
- viene consegnata ai nuovi assunti e messa a disposizione di collaboratori e soggetti esterni rilevanti;

5 – RESPONSABILITÀ

La responsabilità legata alla presente procedura è dell'A.P.S.P. "San Giuseppe" di Primiero, Titolare del Trattamento, il quale si avvale del Direttore per la corretta gestione dei data breach.
Il gruppo di gestione del Data Breach è composto dal Titolare del trattamento, dal Direttore, dal DPO (in qualità di supervisore) e dai referenti delle aree coinvolte.

6 – MODALITÀ OPERATIVE

In caso di accertamento di violazione che rientra nella definizione di "data breach", il Titolare del Trattamento, mediante il Direttore, procede come di seguito dettagliato:

1. provvede all'acquisizione e all'immediata gestione della notizia;
2. compie un'analisi dell'evento;
3. adotta le misure di riduzione del danno;
4. valuta la gravità dell'evento;
5. notifica il "data breach" al Garante Privacy (laddove necessario);
6. procede con la comunicazione agli interessati (se necessario);
7. inserisce l'evento nel proprio Registro delle Violazioni;
8. attiva tutte le azioni correttive per ridurre il ripetersi dell'evento.

Si descrivono di seguito le modalità operative per dare esecuzione a quanto sopra:

1) acquisizione e immediata gestione della notizia

La rilevazione/segnalazione di un data breach può provenire da fonti interne o esterne all'Ente.

- POSSONO ESSERE FONTI INTERNE: notizie ricevute da parte del personale dipendente; da parte del personale convenzionato/stagisti/tirocinanti; dall'amministratore di sistema (ove presente); dalle figure preposte alla manutenzione degli impianti informatici o alla gestione degli archivi; dagli utenti dei servizi.
- SONO FONTI ESTERNE: notizie ricevute da parte delle forze dell'ordine; da parte dei responsabili del trattamento; da parte degli interessati; da parte di terzi.

La segnalazione, qualunque sia la forma, deve essere **immediatamente messa a conoscenza del legale rappresentante dell'Ente, della Direzione, e ove presente, dell'amministratore di sistema**. Tali soggetti, unitamente al DPO e ai referenti delle aree coinvolte, compongono il gruppo di gestione del Data Breach.
La segnalazione deve essere effettuata attraverso canali di posta elettronica (PEC) e avvertimento verbale/telefonico.

2) analisi dell'evento

Il Direttore, nell'immediatezza della rilevazione/segnalazione di un data breach coinvolge il "gruppo di gestione del data breach", e i soggetti in grado di ricostruire le dinamiche dello specifico evento, con i quali compie un'immediata analisi della segnalazione dell'evento riscontrato e/o segnalato per verificare se l'episodio rappresenti effettivamente un "data breach" e mettere in atto, laddove possibile, tutte le appropriate misure per l'immediato contenimento del danno.
L'attività di analisi riguarderà:

- la verifica se la segnalazione dell'episodio riguardi un'ipotesi di violazione dei dati trattati (se di riservatezza, di integrità o di disponibilità);
- l'identificazione dei dati personali violati/distrutti/compromessi e dei relativi trattamenti coinvolti;
- l'identificazione degli interessati;
- il livello di gravità dell'evento;
- le misure di sicurezza presenti sul trattamento coinvolto;
- le immediate azioni che possono essere adottate per ridurre le conseguenze dannose.

Tutte le operazioni effettuate devono essere verbalizzate e la rilevazione della violazione deve contenere almeno i seguenti elementi:

Breve descrizione della violazione dei dati personali	
Quando si è verificata la violazione dei dati personali	
Dove è avvenuta la violazione dei dati	
Dispositivo oggetto della violazione	
Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	
Quante persone sono state colpite dalla violazione dei dati personali	

Che tipo di dati sono oggetto di violazione	
Livello di gravità della violazione dei dati personali	
Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future	

Questa rilevazione deve essere immediatamente trasmessa al DPO mediante i canali di comunicazione istituzionali (posta elettronica - serviziodpo@upipa.tn.it.)

3) valutazione della gravità dell'evento

Il gruppo di gestione del data breach, con il massimo grado di scrupolo e il coinvolgimento di tutte le risorse competenti dovrà verificare se l'evento debba essere notificato al Garante considerando la probabilità o meno che l'evento stesso possa comportare dei rischi per i diritti e la libertà delle persone.

La notifica al Garante è necessaria laddove si sia verificata una violazione (distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati, sia che questi dati siano trattati all'interno che all'esterno dell'Ente) caratterizzata da effetti negativi significativi sulle persone fisiche, che possa causare danni fisici, materiali o immateriali (ad esempio la perdita del controllo da parte degli interessati sui loro dati personali), la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo alle persone fisiche interessate.

Nella attività di valutazione dell'episodio si devono prendere in considerazione **tanto la probabilità quanto la gravità del rischio per i diritti e le libertà degli interessati**. La ponderazione si deve basare sui seguenti elementi di valutazione:

- natura, carattere e volume dei dati personali violati;
- facilità di identificazione delle persone fisiche coinvolte;
- gravità delle conseguenze per le persone fisiche interessate;
- caratteristiche particolari dell'interessato (es. minori, anziani, disabili, ecc.);
- caratteristiche particolari del titolare del trattamento;
- numero delle persone fisiche interessate;
- aspetti generali della violazione.

All'esito dell'analisi, il titolare effettua la notifica al Garante nei termini prescritti (72 ore).

Quando la verifica dei fatti renda "improbabile" che la violazione subita comporti un rischio per i diritti e le libertà delle persone fisiche, la notifica non è obbligatoria ed il titolare deve riportare l'episodio occorso e l'attività di gestione dello stesso nel proprio Registro delle violazioni.

4) notifica della violazione al Garante

La notifica, effettuata dal legale rappresentante o da persona a ciò delegata, verrà portata a compimento nei termini di legge, previa autovalutazione eseguita applicando lo schema accessibile al link

https://servizi.gpdp.it/databreach/s/self-assessment tramite il servizio online disponibile sul sito istituzionale dell'Autorità Garante al link: https://servizi.gpdp.it/databreach/s/scelta-auth.

5) comunicazione agli interessati

In caso di elevato rischio per la libertà e i diritti degli individui, si provvederà ad informare gli interessati tramite i canali istituzionali dell'ente sul fatto avvenuto, sui dati violati e sulle procedure adottate o da adottare per ridurre il rischio.

Nel contesto di tale comunicazione il titolare del trattamento deve fornire agli interessati almeno le seguenti informazioni: una descrizione della natura della violazione; il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto; una descrizione delle probabili conseguenze della violazione; una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

La comunicazione agli interessati non è richiesta laddove il titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi; immediatamente dopo una violazione, il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche; laddove contattare gli interessati richiederebbe uno sforzo sproporzionato.

Copia di ogni comunicazione agli interessati dovrà essere conservata nel Registro delle violazioni.

6) inserimento dell'evento nel Registro delle violazioni

Il Titolare documenta qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.

Il gruppo di gestione del Data Breach è responsabile dell'inserimento di tutte le attività indicate sopra nel Registro delle violazioni, che devono essere documentate, tracciabili, e in grado di fornire evidenza nelle sedi competenti.

7– MATRICE DELLE RESPONSABILITÀ

Attività	Titolare del trattamento A.P.S.P. "San Giuseppe" di Primiero	Direttore Struttura	Personale (Amministrativo, Sanitario, Assistenziale, Servizi Generali)	DPO
1. Segnalazione del sospetto Data Breach	I	I	R (chi rileva segnala)	I
2. Acquisizione e gestione immediata della notizia	C	R	I	I
3. Analisi preliminare dell'evento	C	R	C	I
4. Adozione misure urgenti di contenimento	C	R	C	I
5. Valutazione gravità del rischio	C	R	I	C
6. Notifica al Garante	R	C	I	C
7. Comunicazione agli interessati (se necessaria)	R	C	I	C

Attività	Titolare del trattamento A.P.S.P. "San Giuseppe" di Primiero	Direttore Struttura	Personale (Amministrativo, Sanitario, Assistenziale, Servizi Generali)	DPO
8. Registrazione dell'evento nel Registro delle Violazioni	C	R	I	C
9. Adozione azioni correttive e preventive	R	C	C	C

8 – RIFERIMENTI BIBLIOGRAFICI/NORMATIVI

- REGOLAMENTO (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
- DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n.205) e modifica il D.Lgs 196/03;
- 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.

9 – ALLEGATI/MODULISTICA

- All.1 - FAX SIMILE VERBALE da trasmettere al DPO in caso di DATA BREACH
- All.2 - REGISTRO DELLE VIOLAZIONI