Tipologia Documento	Procedura operativa
Campo di applicazione	Fondazione IRCCS San Gerardo dei Tintori
Processo	A1106
Attività	P22
Struttura emittente	S.C. Affari Generali e Legali - Comitato "Privacy"
Luogo Archiviazione	S.S. Qualità Accreditamento, Internal Auditing e Gestione del Rischio Clinico

Storia delle modifiche

Livello revisione	Data Emissione	Descrizione sintetica delle modifiche apportate
Rev. 0	23.07.2024	Prima emissione

Data 23.07.2024			
Redazione	**Verifica conformità SGQ**	**Iter Approvazione**	
		I Livello	**II Livello**
Coordinatore del gruppo di lavoro	**R. Barni RQA** **Maurizio Pastore- società Liguria Digitale SpA DPO**	**Comitato Privacy**	**Direttore Generale**

Partecipanti al gruppo di lavoro:

Nome Cognome	Ruolo	Struttura
Mariagrazia Meroni	Coordinatore del gruppo di lavoro	SC AGL
Caterina Cerea	Ref. Area QUARC	quarc
Maurizio Pastore-	DPO	società Liguria Digitale SpA

Scopo e campo di applicazione

1. INTRODUZIONE

1.1. Premessa

Per "*Data Breach*" si intende 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*" (Art. 4, par.1, punto 12 del GDPR n. 679/2016, di seguito GDPR).
L'Art. 33 del GDPR recita 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 de idati 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*". La mancata notifica può comportare ulteriori accertamenti da parte dell'Autorità di controllo poiché può rappresentare un indizio di carenze che, se accertate, possono dar luogo a sanzioni.
Con il Provvedimento del Garante sulla notifica delle violazioni dei dati personali (1 luglio 2021) è stato predisposto un modello di notifica al fine di adempiere più agevolmente all'obbligo *ex* art.33 GDPR. Tutti gli eventi di *Data Breach*, compresi quelli per cui non sono necessarie le notifiche, devono essere documentati (Art. 33, par. 5, del GDPR) nel Registro dei *Data Breach.*
A seguito di incidente di sicurezza e sospetta/presunta violazione di dati personali le Strutture coinvolte devono, nell'ambito delle loro competenze, predisporre i mezzi e gli strumenti tecnologici ed organizzativi per:

- individuare la violazione o sospetta violazione;
- analizzare le cause della violazione;
- definire le misure da adottare per rimediare alla violazione dei dati personalie attenuarne i possibili effetti negativi;
- registrare le informazioni relative alla violazione;
- rispondere alle potenziali violazioni dei dati, coinvolgendo anche i fornitori;
- fornire consulenza specialistica nel settore di competenza in supporto ai soggetti identificati come Riceventi.

1.2 Scopo

Scopo della presente procedura è descrivere le azioni da intraprendere in caso di una violazione o sospetta violazione dei dati personali (ex Artt. 33-34 del GDPR n. 679/2016), ponendo particolare attenzione affinché siano effettuati tutti gli sforzi per evitare o limitare i danni e consentire che siano rispettati i tempi richiesti per la segnalazione all'autorità di controllo.

La procedura è applicata dalle seguenti figure:
- Dirigente/ Direttore della Struttura coinvolta;
- S.C. Affari Generali e Legali
- S.C. Sistemi Informativi Aziendali
- DPO;
- Direttore Generale;

2. Responsabilità e gestione del rischio

Attività/fasi	Segnalatore Interno/esterno	**AGL**	**DPO**	**SIA**	**Direzione Generale**	**Accadimento**	**Azione di mitigazione del rischio**	**Area di rischio Tipologia di rischio**
Attivazione: invio segnalazione	R					Mancata/tardiva segnalazione	Aumento dei controlli Formazione del personale	
Presa in carico segnalazione		R	R	R	A	Mancata/tardiva presa in carico Non corretta valutazione dell'evento	Notifica ricezione mail	RISCHIO DI CONFORMITA' (COMPLIANCE)

Attività/fasi	Segnalatore Interno/esterno	**AGL**	**DPO**	**SIA**	**Direzione Generale**	**Accadimento**	**Azione di mitigazione del rischio**	**Area di rischio Tipologia di rischio**
							Presidio dei canali di comunicazione (previsione di più figure preposte per la gestione di eventuali assenze)	TIPOLOGIA NORMATIVA (regionale, nazionale, comunitaria)
Identificare il ruolo Privacy della Fondazione SGT		R	C	R	A	Errata\ incompleta definizione dei ruoli nella documentazione contrattuale e nel Registro dei trattamenti	Formazione del personale Adozione di una procedura/ documentazione per la definizione del ruolo privacy di FSGT Aggiornamento continuo del Registro dei trattamento Audit periodici	RISCHIO DI CONFORMITA' (COMPLIANCE) TIPOLOGIA NORMATIVA (regionale, nazionale, comunitaria)
Effettuare analisi di primo livello		R	R	R	I	Omessa\errata analisi con mancata identificazione dell'evento come data breach	Formazione del personale Revisione della procedura	RISCHIO DI CONFORMITA' (COMPLIANCE) TIPOLOGIA NORMATIVA (regionale, nazionale, comunitaria
Effettuare analisi di secondo livello		R	R	R	I	Omessa\errata analisi deldata breach e classificazione rispetto alla RID	Formazione del personale Revisione della procedura	RISCHIO DI CONFORMITA' (COMPLIANCE) TIPOLOGIA NORMATIVA (regionale, nazionale, comunitaria
Notificare la violazione all'Autorità di controllo		R	C	I	A	Mancato/ritardo invio segnalazione al Garante Privacy	Formazione personale Revisione della procedura Data Breach Gestione della reperibilità del personale per effettuare la notifica entro le 72 ore	RISCHIO DI CONFORMITA' (COMPLIANCE) TIPOLOGIA NORMATIVA (regionale, nazionale, comunitaria)

Attività/fasi	Segnalatore Interno/esterno	**AGL**	**DPO**	**SIA**	**Direzione Generale**	**Accadimento**	**Azione di mitigazione del rischio**	**Area di rischio Tipologia di rischio**
Comunicare la violazione all'Interessato		R	C	C	A	Mancato/ritardo invio segnalazione al Garante Privacy Errore di comunicazione nei confronti dell'interessato	Formazione personale Revisione della procedura Data Breach	RISCHIO DI CONFORMITA' (COMPLIANCE) TIPOLOGIA NORMATIVA (regionale, nazionale, comunitaria)
Documentare la segnalazione-inserimento nel registro data Breach o incidente		R	C	C	A	Mancato aggiornamento Registro Data Breach	Formazione del personale Revisione della procedura Data Breach	RISCHIO DI CONFORMITA' (COMPLIANCE) TIPOLOGIA NORMATIVA (regionale, nazionale, comunitaria)
Identificare aree di miglioramento		R	C	R	A	NA		
Archiviazione documentazione		R			A	Smarrimento	Formazione del personale audit	RISCHIO DI CONFORMITA' (COMPLIANCE) TIPOLOGIA NORMATIVA (regionale, nazionale, comunitaria)

3. Modalità operative

3.1 Attivazione

La procedura viene attivata da chiunque venga a conoscenza o sospetti un incidente di sicurezza e/o violazione di dati personali a seguito di comunicazione preliminare agli indirizzi e-mail: privacy@irccs-sangerardo.it, dpo@irccs-sangerardo.it e a segreteria.sia@irccs-sangerardo.it.

La segnalazione può pervenire da:

- **canali interni**
  - da chiunque all'interno della Fondazione SGT rilevi o sospetti una violazione di dati personali;
  - dal DPO in quanto punto di contatto primario per gli interessati;
  - dal Direttore della S.C. Sistemi Informativi Aziendali nel caso in cui un incidente di sicurezza informatica comporti una violazione di dati personali.
- **canali esterni**
  - segnalazione dell'interessato;
  - segnalazione da parte dei fornitori;

- segnalazione da parte di ulteriori soggetti;
- segnalazione da parte degli Organi Pubblici (AgID, Polizia, altre Forze dell'Ordine, giornalisti, ecc.).

All'arrivo di una segnalazione devono essere attuate le prime azioni per il contenimento dell'incidente occorso. A titolo esemplificativo: in caso di accesso non autorizzato ai sistemi è consigliato cambiare la password di accesso; in caso di perdita dei dati è necessario verificare se sono stati effettuati dei back up al fine di ripristinare al più presto i dati; in caso di furto di documentazione occorre verificare che siano state messe in atto opportune misure di sicurezza come la chiusura a chiave di una stanza o la presenza di un lucchetto.

3.2 Passi procedurali

3.2.1 Segnalare il sospetto incidente e/o violazione

Fermo restando quanto previsto dal Modello organizzativo privacy (MOP), con particolare riguardo all'identificazione dei ruoli privacy all'interno della Fondazione, a seguito della rilevazione del sospetto incidente e/o violazione, le Strutture coinvolte comunicano l'evento alla S.C. Affari Generali e Legali, alla S.C. Sistemi Informativi Aziendali e al DPO, tramite il modello allegato alla presente procedura (A1106_P22_P02_M01).

L'analisi preliminare ha come obiettivo quello di raccogliere tutte le informazioni relative all' evento segnalato:

a) data e ora;
b) fonte;
c) tipologia dell'evento e descrizione;
d) stima del numero interessati coinvolti;
e) stima della numerosità dei dati personali di cui si presume la violazione;
f) luogo in cui è avvenuta la violazione o presunta violazione;
g) descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti,con indicazione della loro ubicazione.

Nel caso in cui la segnalazione pervenuta riguardi trattamenti di dati personali gestiti dalla Fondazione SGT in qualità di Responsabile ex art. 28 del GDPR, si procede come descritto al paragrafo 3.2.8 "Gestire la segnalazione in qualità di Responsabile".

Nel caso in cui la segnalazione pervenuta riguardi trattamenti di dati personali svolti dalla Fondazione SGT in qualità di Titolare si procede con i passi seguenti.

La segnalazione è sottoscritta dal Direttore/Responsabile della struttura segnalante.

3.2.2 Effettuare analisi di primo livello

Il DPO, la S.C. Sistemi Informativi Aziendali e la S.C. Affari Generali e Legali avviano **l'analisi di primo livello**.

L'analisi di primo livello ha come obiettivo quello di verificare che la segnalazione non sia un falso positivo, ovvero che l'evento non abbia comportato la violazione di dati personali.

Nel caso in cui l'evento segnalato risulti essere un falso positivo, si chiude l'incidente e la S.C. Sistemi Informativi Aziendali si attiva per effettuare un raffinamento delle regole di rilevazione dei falsi positivi; quindi, si procede come descritto al paragrafo 3.2.6 "Documentare la segnalazione".

Nel caso la violazione dei dati personali venga accertata, si passa alla fase di analisi di secondo livello.

3.2.3 Effettuare analisi di secondo livello

L'analisi di **secondo livello** deve essere effettuata nel più breve tempo possibile dall'avvenuta conoscenza dell'evento.

Il DPO, la S.C. Sistemi Informativi Aziendali e la S.C. Affari Generali e Legali devono identificare:

- **categoria di violazione:**

- perdita di riservatezza;
- perdita di integrità;
- perdita di disponibilità;

- **supporto oggetto della violazione** (es. applicativo, banche dati, servizi serverfarm, dispositivo mobile, computer, documento cartaceo, etc.);
- **dati oggetto della violazione e i relativi trattamenti censiti nel Registro dei trattamenti;**
- **Interessati;**
- **il contenimento del danno come di seguito descritto:**
  - limitazione o annullamento degli effetti dell'incidente;
  - raccolta delle prove forensi nel caso sia ipotizzato un reato;
  - determinazione delle azioni possibili di ripristino, ed avvio delle stesse;
  - ripristino dei dati, dei sistemi, dell'infrastruttura e delle configurazioni;
  - valutazione dei tempi di ripristino;
  - verifica dei sistemi recuperati;
  - valutazione delle eventuali vulnerabilità collegate con l'incidente;
  - individuazione delle azioni di mitigazione delle vulnerabilità individuate.

Per facilitare la classificazione del rischio per i diritti e le libertà fondamentali delle persone fisiche, la violazione può essere valutata secondo i livelli di rischio riportati da ENISA (The European Union Agency for Cybersecurity).

L'analisi dei Rischi elaborata da ENISA prende in considerazione i seguenti parametri:

- contesto del trattamento e tipologia di dati;
- facilità di identificazione dell'individuo sulla base dei dati violati;
- circostanze della violazione.

In base a tali parametri si calcola un livello di rischio attraverso la seguente formula:

Rischio = (Contesto x Facilità di identificazione) + Circostanze

Il risultato ottenuto permette la seguente catalogazione dei livelli di rischio:

a) **Basso (<2)**: gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (Es. tempo trascorso reinserendo informazioni, fastidi, irritazioni, etc.).
b) **Medio (tra 2 e 3)**: gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (Es. costi aggiuntivi, rifiuto di accesso ai servizi della Fondazione SGT, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, etc.).
c) **Alto (tra 3 e 4)**: gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (Es. appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, etc.).
d) **Molto alto (>4)**: gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Saranno inoltre valutate, come variabili qualitative dell'impatto temuto, le seguenti eventuali condizioni:

a) che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
b) che si tratti di dati relativi a valutazione di aspetti personali, in particolare mediante l'analisi o la 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;

c) che si tratti di dati di persone fisiche vulnerabili, in particolare minori;
d) che il trattamento riguardi una notevole quantità di dati personali;
e) che il trattamento riguardi un vasto numero di interessati.

3.2.4 Notificare la violazione all'Autorità di controllo

Qualora, dopo l'analisi di secondo livello, risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, non è necessario procedere con la notifica all'Autorità di controllo.

La documentazione prodotta in fase di analisi e corredata dalle relative motivazioni andrà inserita nel Registro dei *Data Breach* a cura della S.C. Affari Generali e Legali.

Nei casi in cui sussista un maggiore livello di rischio il Dirigente/ Direttore della Struttura coinvolta, la S.C. Affari Generali e Legali, la S.C. Sistemi Informativi Aziendali, il DPO ed il Direttore Generale devono valutare le azioni da intraprendere ed effettuare la notifica all'Autorità di controllo, tramite il modello presente sul sito del Garante pe la protezione dei dati personali. Laddove necessario, devono provvedere alla comunicazione agli interessati, verificando e validando la documentazione pervenuta dalle precedenti fasi di lavoro.

La notifica all'Autorità di controllo deve essere effettuata nel caso in cui i rischi per le persone fisiche non siano trascurabili e solo nel caso in cui la Fondazione SGT sia Titolare del/i trattamento/i dei dati coinvolti nella violazione.

La notifica all'autorità di controllo deve descrivere, ove possibile:

- la natura della violazione dei dati personali compresi;
- le categorie e il numero approssimativo di interessati in questione;
- le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- il nome e i dati di contatto del DPO;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate, o di cui si propone l'adozione da parte della Fondazione SGT, per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora non sia possibile fornire fin da subito le informazioni, possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

3.2.5 Comunicare la violazione all'Interessato

Le strutture coinvolte, con il supporto della S.C. Affari Generali e Legali e la S.C. Sistemi Informativi Aziendali e del DPO devono informare gli interessati dell'evento anomalo, in tutti i casi in cui, a norma degli artt. 33-34 GDPR, la violazione presenta gravi rischi per i diritti e le libertà delle persone fisiche.

La comunicazione deve essere rivolta all'interessato senza ingiustificato ritardo dall'avvenuta conoscenza e valutazione della violazione, attraverso il canale di comunicazione ritenuto più idoneo.

La comunicazione deve essere intellegibile, concisa, trasparente e facilmente accessibile. Deve essere utilizzato un linguaggio semplice e chiaro adottando, se possibile, la stessa lingua parlata dall'interessato.

La comunicazione di *Data Breach* all'interessato deve contenere le seguenti informazioni:

- data e ora della violazione, anche solo presunta, e data e ora in cui si è avuta conoscenza della stessa;
- la natura della violazione dei dati personali;
- il nome e i dati di contatto del DPO;
- le probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o di cui si propone l'adozione da parte della Fondazione SGT a per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

- 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, salvo i casi in cui la violazione della sicurezza ha comportato la distruzione o la perdita dei dati personali degli interessati;

- sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà delle persone fisiche; in tal caso è necessario documentare le misure nel Registro e nella comunicazione all'Autorità di controllo;
- detta comunicazione richiederebbe sforzi sproporzionati; in tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

La Fondazione SGT deve effettuare la comunicazione nelle casistiche descritte in precedenza e solo per i trattamenti in qualità di Titolare del Trattamento.

3.2.6 Documentare la segnalazione

L'Art. 33 del GDPR prescrive al Titolare del trattamento di documentare qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.

Nel Registro dei *Data Breach* viene documentato ogni singolo evento, sia esso falso, irrilevante o rilevante; in quest'ultimi due casi, devono essere indicate nel Registro:

- le conseguenze del Data Breach;
- i provvedimenti adottati per porvi rimedio o attenuarne le conseguenze;
- l'eventuale notifica all'Autorità di controllo;
- l'eventuale comunicazione all'Interessato.

Nel Registro vanno inserite tutte le segnalazioni di violazione pervenute alla Fondazione SGT sia come Titolare del trattamento, sia come Responsabile del trattamento.

Per quanto riguarda la documentazione delle violazioni, il Titolare del trattamento tiene conto del parere del DPO in merito alla struttura, all'impostazione e all'amministrazione della documentazione stessa.

3.2.7 Identificare le aree di miglioramento

Le azioni di miglioramento previste in fase di applicazione della presente procedura sono le seguenti:

a) Analisi dell'evento con figure tecniche-professionali competenti per individuare le vulnerabilità;
b) adozione di nuovi sistemi tecnici di prevenzione/protezione e/o di sistemi di controllo/monitoraggio/allarme;
c) individuazione di controlli e misure di sicurezza che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
d) valutazione su possibilità di copertura assicurativa;
e) azioni informative rivolte ai dipendenti;
f) revisione delle relazioni con i Fornitori;
g) pianificazione dei test periodici per verificare la validità della presente procedura;
h) revisione della procedura, se necessario, e di eventuali altri documenti collegati.

3.2.8 Gestire la segnalazione in qualità di Responsabile

Nei casi in cui la Fondazione SGT agisca come Responsabile del trattamento di dati personali, la suddetta deve comunicare l'incidente di sicurezza riguardante i dati personali al Titolare con le modalità convenute negli atti di nomina/istruzioni ricevute e con la massima tempestività, fornendo tutte le informazioni necessarie e mettendosi a disposizione di quest'ultimo per approfondimenti e contenimento dei danni.

L'Azienda non ha il dovere di notificare all'autorità Garante quando agisce come Responsabile del trattamento per conto di altro Titolare (senza delega alla notifica al Garante). Spetta infatti al Titolare la valutazione dell'effettiva sussistenza della violazione di dati personali.

Anche la comunicazione verso l'Interessato, nei casi in cui Fondazione SGT agisca in qualità di Responsabile spetta al Titolare.

L'incidente di sicurezza riguardante i dati personali va, comunque, documentato come descritto al paragrafo 3.3.6 "Documentare la segnalazione".

4. Indicatori

Num. Notifiche di segnalazione data breach al Garante della privacy entro 72 ore / num. tot. Segnalazioni data breach

Frequenza della rilevazione: Annuale
Resp. Rilevazione: AGL
Valore soglia >90%

5. Documenti di riferimento o Bibliografia o Sitografia

- Art. 4,33,34, 55 del GDPR (General Data Protection Regulation) n. 679/2016;
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (*data breach*),;
- Linee Guida sulla notifica delle Violazioni dei dati personali ai sensi del Regolamento UE 2016/679 - WP 250 Versione emendata e adottata in data 6 febbraio 2018 (Gruppo di lavoro europeo Art. 29 per la protezione dei dati);
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali dell'1 luglio 2021;
- www.gpdp.it.

6. Allegati

A1106_P22_M01 Modello di comunicazione da trasmettere a seguito di rilevazione del sospetto incidente e/o della violazione all'attenzione della S.C. Affari Generali e Legali, alla S.C. Sistemi Informativi Aziendali e al DPO.

7. Acronimi

- AgID: Agenzia per l'Italia Digitale
- DPO: Data Protection Officer
- GDPR: General Data Protection Regulation (Regolamento europeo n. 679/2016)
- PEC: Posta Elettronica Certificata
- SIA: Sistemi Informativi Aziendali

La presente procedura sarà oggetto di valutazione periodica al fine di verificarne l'effettiva efficacia, nonché di revisione e/o di aggiornamento in virtù degli esiti della predetta attività valutativa ovvero a seguito dell'entrata in vigore di provvedimenti legislativi o regolamentari che richiedano il suo adeguamento.

Legenda

R (Responsable) – Responsabile dell'esecuzione dell'attività è il ruolo di colui che è chiamato ad eseguire operativamente l'attività (per ogni attività è possibile avere più Responsabili).

A (Accountable) – Responsabile sul risultato dell'attività è solitamente il ruolo di supervisione del lavoro del/dei Responsabile (deve essere univocamente individuato).

C (Consult) – è il ruolo di chi dovrà supportare il/i Responsabile/i nello svolgimento dell'attività fornendo informazioni utili al completamento del lavoro o a migliorare la qualità del lavoro stesso.

I (Inform) – è il ruolo di chi dovrà essere informato in merito al lavoro del/dei Responsabile/i e che dovrà, se necessario, prendere decisioni sulla base delle informazioni avute.