Allg. 4

Procedura per la gestione del Data Breach

Storia del documento

Data	Versione	Descrizione modifiche	Autore
20/02/2019	1.0	Prima emissione	

44

Sommario

Indice delle figure

45

Indice delle tabelle

1 Introduzione

Il Regolamento UE 2016/679 (di seguito "Regolamento" o "GDPR") [1] è mirato alla protezione dei dati personali, ovvero ad evitare che possano essere violati diritti e libertà degli interessati.

Come richiesto dal Regolamento, l'Azienda Sanitaria Locale di Salerno (di seguito "ASL di Salerno") si impegna a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e, in caso di violazione dei dati stessi, ad intraprendere misure correttive e cautelative verso gli interessati senza ingiustificato ritardo, effettuando ove necessario e previsto dalla normativa, la notifica al Garante per la protezione dei dati personali (di seguito "Garante") e l'eventuale comunicazione agli interessati.

In linea con la definizione fornita dal GPDR (art. 4 par.12), la violazione dei dati personali è 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"*.

Come specificato anche dal Gruppo di lavoro Articolo 29 per la protezione dei dati [7], una violazione dei dati personali (di seguito anche "Data Breach") può compromettere:

- La riservatezza (divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali);
- L'integrità (modifica non autorizzata o accidentale dei dati personali);
- La disponibilità (perdita, accesso o distruzione accidentali o non autorizzati di dati personali);
- Una combinazione dei fattori precedentemente elencati.

Una violazione dei dati personali può riguardare:

- Un trattamento di natura informatica che impatta, o comunque vede coinvolti, sistemi informatici;
- Un trattamento che riguarda la documentazione cartacea;
- Una combinazione dei punti precedenti.

Di seguito alcuni esempi di violazioni di dati personali:

- Accesso o acquisizione dei dati da parte di terzi non autorizzati;
- Furto o perdita di dispositivi informatici contenenti dati personali;
- Furto o perdita di documentazione cartacea contenente dati personali;
- Deliberata alterazione di dati personali;
- Impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;

47

- Perdita o distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- Divulgazione non autorizzata dei dati personali.

1.1 Finalità del documento

Il presente documento ha l'obiettivo di descrivere, in maniera chiara e comprensibile da tutto il personale della ASL di Salerno, processi, modalità operative, ruoli e responsabilità organizzative, che consentano un approccio esaustivo ed omogeneo nella gestione delle violazioni di sicurezza relative ai dati personali, secondo i criteri ed i principi stabiliti dalle vigenti normative ed in accordo alla "Linee guida per la gestione delle violazioni della sicurezza dei dati personali" [8] della ASL di Salerno.

1.2 Ambito di applicazione

La procedura operativa si applica, nello specifico, a tutto il personale dell'Struttura Sanitaria che tratta a qualsiasi titolo e in qualsiasi modalità (digitale, cartacea, etc.) dati personali e, ove applicabile, alle terze parti che operano per conto della ASL di Salerno.

1.3 Documenti di riferimento

[1] Regolamento (UE) 2016/679 del Parlamento Europeo 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 particolare gli articoli 33 (Notifica all'Autorità di Controllo), 34 (notifica agli interessati) e 28 (Responsabile del trattamento)

[2] D.Lgs. 30 Giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"

[3] Decreto Legislativo 10 agosto 2018 n, 101 "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)"

[4] ISO/IEC 27001:2013 "Information Security Management Systems", 01/10/2013

[5] ISO/IEC 27002:2013 "Code of practice for information security controls", 01/10/2013

[6] ISO/IEC 29134:2017(E) "Information technology - Security techniques - Guidelines for privacy impact assessment", First edition 2017-06

[7] "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679", WP250, rev. 0.1, 06/02/2018

[8] "Linee guida per la gestione delle violazioni della sicurezza dei dati personali" della ASL Salerno

1.4 Acronimi e Definizioni

ASL	Azienda Sanitaria Locale
Autorità di controllo	L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR. Il Decreto Legislativo 10 agosto 2018 n, 101 [3] individua l'Autorità di controllo nel Garante per la protezione dei dati personali.
Categorie particolari di dati personali	Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Contitolare del trattamento	Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento.
Criticità	Insieme di circostanze avverse, derivanti dalla concomitanza di eventi che costituiscono una minaccia per la sicurezza e la privacy di un determinato contesto.
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.
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
Evento	Qualsiasi occorrenza che si verifica nell'ambito di un determinato asset informativo, rilevata mediante strumenti automatizzati o non automatizzati, la cui valenza è considerata significativa ai fini delle attività di gestione, controllo della privacy e contenimento dei rischi ad essa correlati.
Falso positivo	Evento o insieme di eventi che, pur essendo stati segnalati come manifestazioni di possibili violazioni della privacy, non rivestono carattere di rilevanza nello specifico contesto entro il quale si sono verificati.

GDPR	Regolamento Generale per la Protezione dei Dati.
Pseudonimizzazione	Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
Responsabile del Trattamento	Persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento.
SIA	Sistema Informativo Aziendale
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.
UOC	Unità Operativa Complessa
Violazione dei dati personali	La 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.

1.5 Ruoli e responsabilità

Di seguito sono descritti i principali ruoli e responsabilità nel processo di gestione delle violazioni di dati personali (Data Breach) oggetto della presente procedura.

1.5.1 Ruoli

Oltre ai ruoli istituzionali del Titolare del trattamento (di seguito anche "Titolare") e del DPO, nell'ambito della presente procedura si identificano i seguenti ruoli:

- Il ruolo di **Referente della Segnalazione**, che può essere ricoperto da:
  - Soggetto interno (dipendente, collaboratore interno), in particolare la UOC SIA che gestisce i sistemi di monitoraggio ed allarmistica relativi ad eventi ICT;
  - Soggetto esterno (Responsabile del trattamento, Contitolare, Organi Istituzionali, Interessati, etc.);
- Il ruolo di **Comitato Data Breach**, che è ricoperto da:
  - Titolare;
  - DPO;
  - Responsabili dell'Area Direzionale (Direzione Generale, Direzione Amministrativa, Direzione Sanitaria);
  - Responsabili dell'Area Clinico-Assistenziale;
  - Responsabili dell'Area Amministrativa e Tecnica;
  - Responsabile del Team di Gestione Data Breach;
- Il ruolo di **Team di Gestione Data Breach**, che è ricoperto da:
  - Referenti dell'Area Direzionale (Direzione Generale, Direzione Amministrativa, Direzione Sanitaria);
  - Referenti dell'Area Clinico-Assistenziale;
  - Referenti dell'Area Amministrativa e Tecnica;
- Il ruolo di **Responsabile del Team di Gestione Data Breach**, che è ricoperto da:
  - Direttore dell'UOC SIA.

1.5.2 Responsabilità

In relazione ai ruoli sopra definiti, si identificano le seguenti responsabilità:

- Il **Titolare del Trattamento** ha la responsabilità di:
  - Supervisionare le attività svolte dal Comitato Data Breach e fungere da organo decisionale per il Comitato e per tutte le attività descritte nella presente procedura ove richiesto;

51

- Compilare e inviare la notifica al Garante, se è stato accertato che la violazione può comportare un rischio per i diritti e le libertà delle persone fisiche;
- Compilare e inviare la comunicazione agli Interessati, se è stato accertato che la violazione può comportare un rischio elevato per i diritti e le libertà delle persone fisiche;

- Il **DPO** ha la responsabilità di:
  - Verificare la correttezza formale della segnalazione di violazione dei dati personali;
  - Attivare il Responsabile del Team di Gestione Data Breach;
  - Supervisionare le attività di gestione Data Breach e fungere da organo consultivo per tutte le attività descritte nella presente procedura;
  - Svolgere i compiti assegnati al Comitato Data Breach, in qualità di membro dello stesso;
  - Cooperare con il Garante e fungere da punto di contatto per quest'ultimo e per gli interessati;
  - Verificare quanto emerso dalla "root cause analysis" delle violazioni di dati personali ed indirizzare di concerto con il Responsabile del Team di Gestione Data Breach le azioni di miglioramento;
- Il **Referente della Segnalazione** ha la responsabilità di:
  - Segnalare ogni violazione dei dati personali (presunta o accertata) con le modalità ed i tempi descritti nella presente procedura;
- Il **Comitato Data Breach** ha la responsabilità di:
  - Verificare l'analisi e la classificazione effettuate dal Team di Gestione Data Breach;
  - Effettuare la valutazione del Data Breach identificandone la classe di rilevanza.
- Il **Team di Gestione Data Breach** ha la responsabilità di:
  - Effettuare l'analisi e la classificazione dell'evento segnalato come violazione di dati personali;
  - Identificare ed attuare le azioni di contrasto e recupero;
  - Supportare il Comitato nella fase di valutazione del Data Breach;
  - Predisporre e mantenere aggiornato il "Registro Eventi e Violazioni Privacy" con le informazioni raccolte durante le varie fasi del processo;
  - Condurre la "root cause analysis" delle violazioni di dati personali;
- **Responsabile del Team di Gestione Data Breach** ha la responsabilità di:
  - Attivare il Team di Gestione Data Breach ed il Comitato Data Breach nei casi previsti dalla presente procedura, coinvolgendo opportunamente i referenti competenti in relazione alle informazioni disponibili sull'evento;
  - Supervisionare le attività svolte dal Team di Gestione Data Breach e fungere da organo decisionale per il Team;

- Verificare quanto emerso dalla "root cause analysis" delle violazioni di dati personali ed indirizzare di concerto con il DPO le azioni di miglioramento.

2 Procedura Operativa per la Gestione di Data Breach

Il processo di gestione del Data Breach adottato dalla ASL di Salerno prevede le seguenti fasi:

- Rilevazione e Segnalazione Evento;
- Analisi e Classificazione Evento;
- Contrasto e Recupero;
- Valutazione Data Breach;
- Notifica al Garante (ove necessario);
- Comunicazione agli Interessati (ove necessario);
- Miglioramento Continuo.

Nei paragrafi successivi sono descritte nel dettaglio le singole fasi.

2.1 Rilevazione e Segnalazione Evento

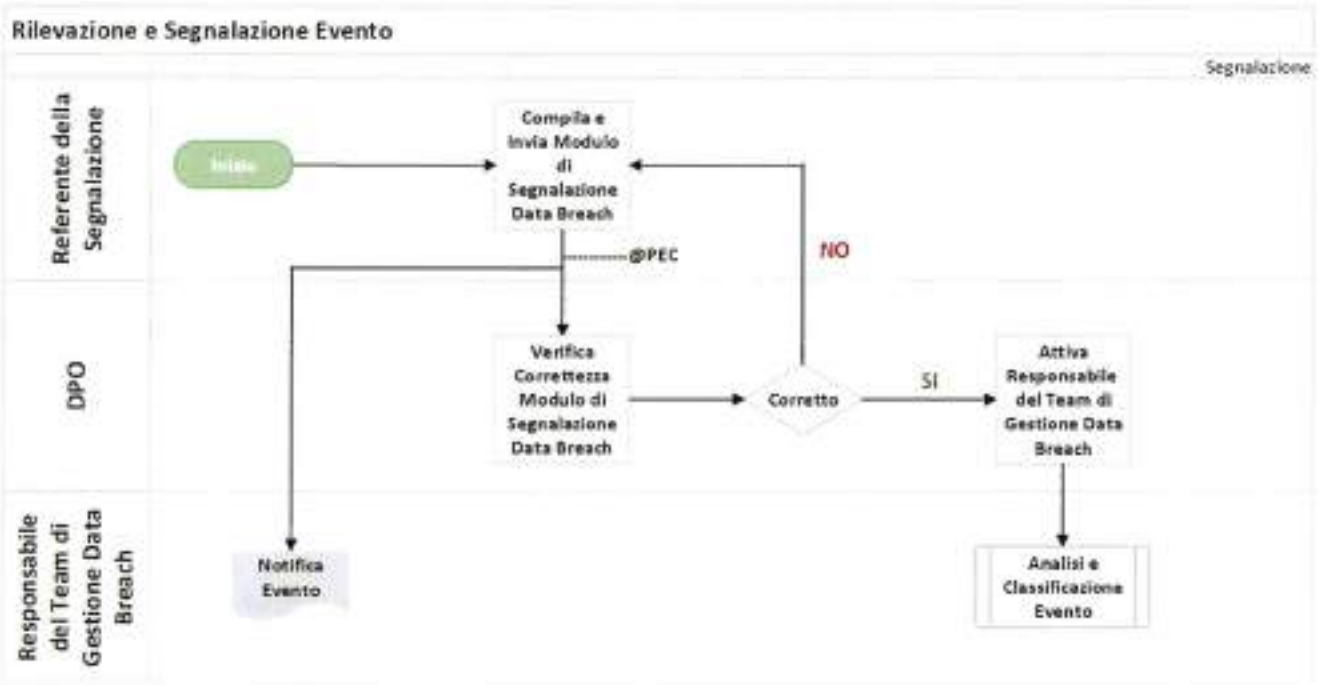

Figura 1 – Rilevazione e Segnalazione Evento

Ogni violazione di dati personali (potenziale o accertata) deve essere tempestivamente comunicata alla **casella PEC del DPO** nel tempo massimo di **1 ora**, dopo esserne venuti a conoscenza, allegando il "Modulo di segnalazione Data Breach" opportunamente compilato.

53

Tale modulo è fornito in allegato (cfr. par. 3.1) alla presente procedura e disponibile sul sito Internet della ASL di Salerno.

Il DPO deve in ogni caso essere avvisato anche verbalmente o telefonicamente.

La **casella PEC del DPO** è configurata in modo da effettuare un inoltro automatico al Responsabile Team di Gestione del Data Breach.

Ricevuta la segnalazione, il DPO effettua la verifica del modulo ricevuto contattando se necessario il Referente della Segnalazione per eventuali chiarimenti/integrazioni rispetto a quanto riportato nel modulo. Completata la verifica, il DPO attiva tempestivamente il Responsabile del Team di Gestione Data Breach per avviare la fase successiva di Analisi e Classificazione Evento (cfr. par. 2.2).

Dal momento in cui i soggetti preposti vengono a conoscenza dell'evento, decorre il termine delle 72 ore previsto dalla normativa per l'invio della notifica al Garante per la protezione dei dati personali quando dovuto.

2.2 Analisi e Classificazione Evento

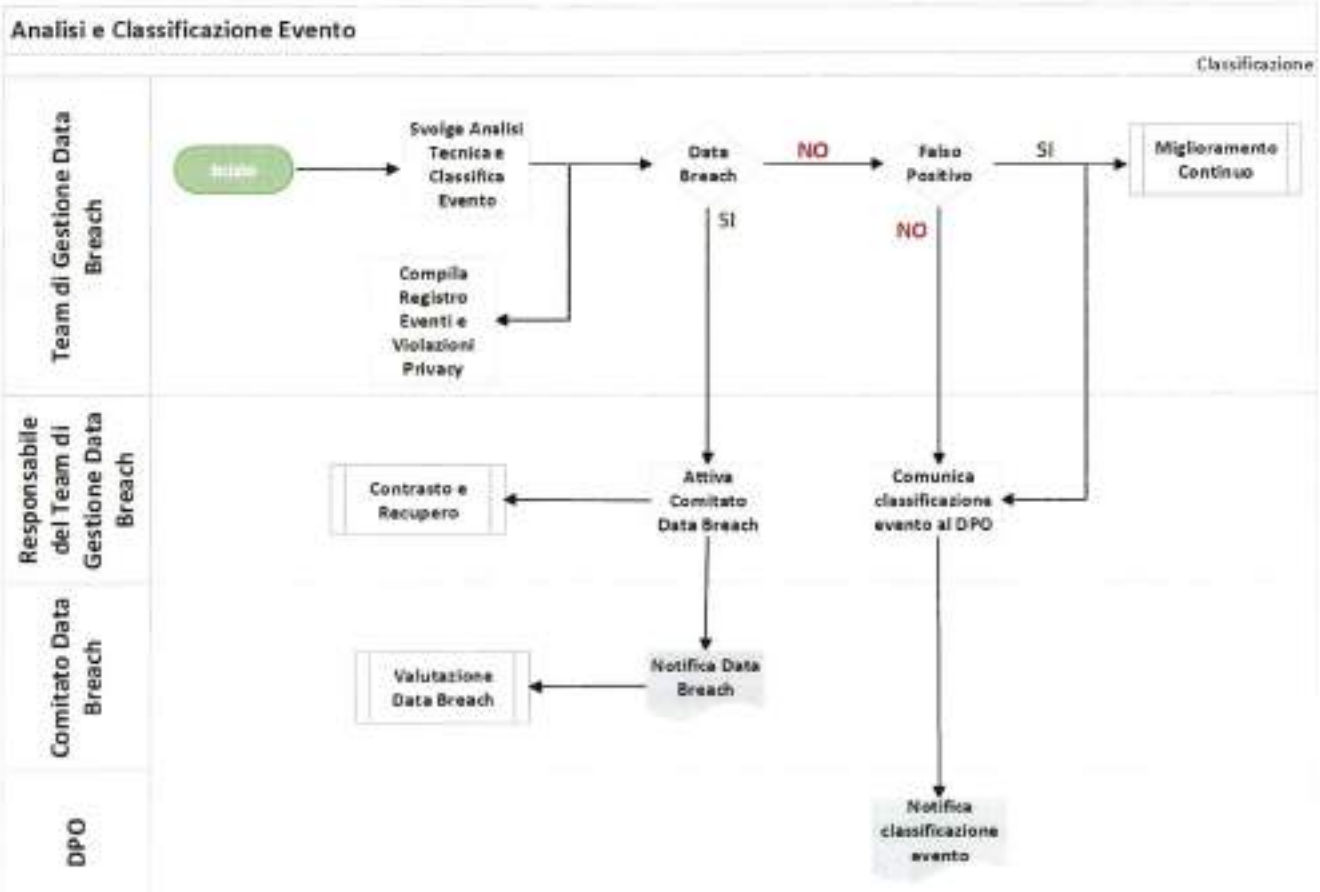

Figura 2 – Analisi e Classificazione Evento

In tale fase il Responsabile del Team di Gestione Data Breach coinvolge opportunamente i referenti del Team competenti in base alle specificità dell'evento.

Sotto il coordinamento del Responsabile del Team di Gestione Data Breach, il Team di Gestione Data Breach svolge le seguenti attività:

- Analisi tecnica dell'evento, utilizzando il modulo compilato dal Referente della Segnalazione e raccogliendo ulteriori informazioni;
- Classificazione dell'evento, al fine di indirizzare tempestivamente le azioni di contrasto e recupero (cfr. par. 2.3), nonché attivazione se necessario del Comitato Data Breach;
- Inserimento delle informazioni relative all'evento nel "Registro Eventi e Violazioni Privacy" secondo il "Modulo di Registro Eventi e Violazioni Privacy" fornito in allegato (cfr. par. 5.5), compilando i campi inerenti alle fasi "Rilevazione e Segnalazione evento" e "Analisi e Classificazione Evento".

In particolare, il Team documenta le attività di analisi e classificazione svolte riportando nel Registro Eventi e Violazioni Privacy le seguenti informazioni:

- "**Asset coinvolti**", elenco degli asset coinvolti (computer, tablet, base dati, documento cartaceo, chiavetta USB, apparato elettromedicale, etc.) fornendo indicazioni puntuali;
- "**Trattamenti coinvolti**", elenco dei trattamenti interessati dall'evento, prendendo come riferimento la nomenclatura utilizzata nel Registro dei Trattamenti della Struttura Sanitaria;
- "**Criticità Trattamenti**", utilizzando la scala valutativa a tre livelli (Bassa, Media, Alta) in linea con la "Politica per la classificazione dei trattamenti e delle informazioni". Nel caso in cui siano presenti trattamenti con diversi livelli di criticità, il giudizio di criticità deve essere ricondotto al valore massimo tra i livelli dei trattamenti;
- "**Tipologia dati personali**", tipologia di dati personali interessati dall'evento, utilizzando la medesima tassonomia utilizzata nel Registro dei Trattamenti della Struttura Sanitaria;
- "**Categoria di interessati coinvolti e numerosità**", tipologia di interessati coinvolti nell'evento, prendendo come riferimento la nomenclatura utilizzata nel Registro dei Trattamenti della Struttura Sanitaria e numerosità stimata o accertata;
- "**Misure di sicurezza adottate**", descrizione delle misure di sicurezza adottate a protezione dei dati (tecniche di cifratura, pseudonimizzazione, etc.);
- "**Classificazione Evento**", tipologia di evento secondo la seguente nomenclatura:
  - **Data Breach**, evento che sottintende una violazione della privacy;
  - **Falso Positivo**, evento teoricamente malevolo che tuttavia non comporta alcuna violazione della privacy nel contesto specifico in esame;
  - **Fuori Ambito Privacy**, evento non riguardante i dati personali e quindi fuori dall'ambito della presente procedura;

55

- **"Descrizione Impatto Privacy"**, solo nel caso di evento classificato come Data Breach, descrizione delle possibili conseguenze per gli interessati coinvolti;
- **"Impatto Privacy"**, solo nel caso di evento classificato come Data Breach, giudizio (classificazione) relativamente ai possibili impatti sui diritti e sulle libertà degli interessati riconducibili all'evento, utilizzando la seguente scala valutativa:
  - **Grave**: giudizio che sottintende una violazione della privacy causa di danni permanenti e non reversibili alla riservatezza, integrità e disponibilità dei dati personali e/o dei trattamenti;
  - **Rilevante**: giudizio che sottintende una violazione della privacy causa di danni temporanei e reversibili alla riservatezza, integrità e disponibilità dei dati personali e/o dei trattamenti;
  - **Significativo**: giudizio che sottintende una violazione della privacy che non comporta danni permanenti o temporanei tali da compromettere la riservatezza, integrità e disponibilità dei dati personali e/o dei trattamenti;
- **"Criticità Data Breach"**, utilizzando la scala valutativa a tre livelli (Bassa, Media, Alta), determinata sulla base dell'Impatto Privacy e della Criticità del trattamento, secondo la seguente tabella decisionale.

Tabella per la valutazione di criticità del Data Breach		
Impatto privacy	**Criticità trattamento**	**Criticità del Data Breach**
GRAVE	ALTA	ALTA
RILEVANTE	ALTA	ALTA
SIGNIFICATIVO	ALTA	MEDIA
GRAVE	MEDIA	ALTA
RILEVANTE	MEDIA	ALTA
SIGNIFICATIVO	MEDIA	MEDIA
GRAVE	BASSA	ALTA
RILEVANTE	BASSA	MEDIA
SIGNIFICATIVO	BASSA	BASSA

Tabella 1 - Tabella per la valutazione di criticità del Data Breach

Nella descrizione dell'Impatto Privacy occorre specificare quali impatti possono realizzarsi o si sono realizzati, prendendo come riferimento il seguente elenco (indicativo, ma non esaustivo):

- Danno fisico, materiale o psicologico; (cfr. "Linee guida per la conduzione delle attività di Data Protection Impact Assessment");
- 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 della pseudonimizzazione;
- 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.

Nei casi di evento classificato come "Fuori Ambito Privacy" o "Falso Positivo", il Responsabile del Team di Gestione Data Breach comunica a mezzo e-mail tale classificazione al DPO.

Per l'evento "Fuori Ambito Privacy" sono seguite le specifiche procedure interne della Struttura Sanitaria, mentre il "Falso Positivo" viene successivamente analizzato nella fase di Miglioramento Continuo (cfr. par. 2.7).

Nel caso di evento classificato come "Data Breach", il Responsabile del Team di Gestione Data Breach avvia le eventuali azioni di contrasto e recupero (cfr. par. 2.3) e attiva il Comitato Data Breach per la fase successiva di Valutazione del Data Breach (cfr. par. 2.4).

Il Team di Gestione Data Breach inserisce nella sezione specifica del "Registro Eventi e Violazioni Privacy" le informazioni legate a tale fase.

2.3 Contrasto e Recupero

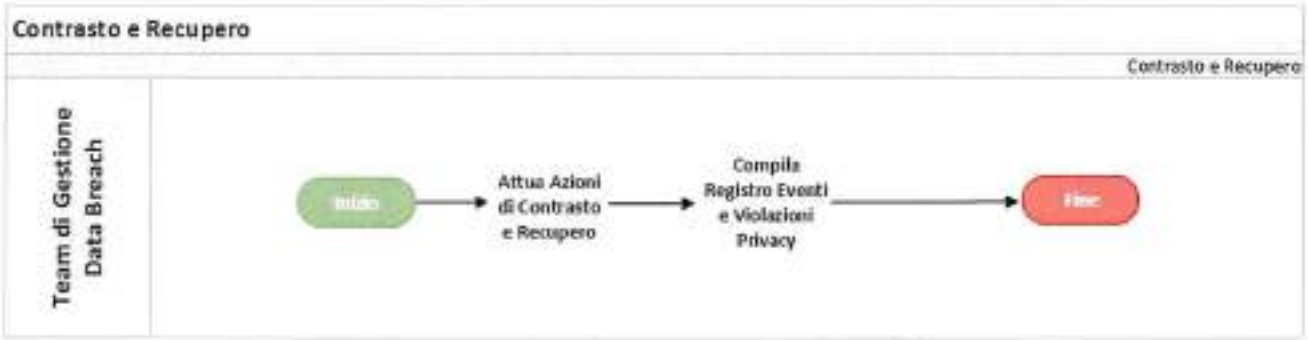

Figura 3 – Contrasto e Recupero

In base alla criticità dell'evento il Team di Gestione Data Breach si attiva per avviare le attività di contrasto e recupero secondo la seguente tempistica:

- Se il Data Breach ha criticità **Bassa**, le azioni di contrasto e recupero devono essere avviate **entro 6 ore** dal rilevamento dell'evento;
- Se il Data Breach ha criticità **Media**, le azioni di contrasto e recupero devono essere avviate **entro 4 ore** dal rilevamento dell'evento;
- Se il Data Breach ha criticità **Alta**, le azioni di contrasto e recupero devono essere avviate **entro 2 ore** dal rilevamento dell'evento.

Il Team di Gestione Data Breach avvia, entro i tempi di cui sopra, le seguenti azioni:

- Limitazione degli effetti della violazione;

- Determinazione delle azioni possibili di ripristino;
- Valutazione delle eventuali vulnerabilità collegate con la violazione;
- Individuazione delle azioni di mitigazione delle vulnerabilità individuate;
- Valutazione dei tempi di ripristino;
- Eventuale gestione dei contatti con i Responsabili del Trattamento e con le funzioni della Struttura Sanitaria per l'attuazione delle azioni individuate;
- Ripristino dei dati, dei sistemi, dell'infrastruttura e delle configurazioni;
- Verifica dei sistemi recuperati.

Il Team di Gestione Data Breach inserisce nella sezione specifica del "Registro Eventi e Violazioni Privacy" le informazioni legate a tale fase.

2.4 Valutazione Data Breach

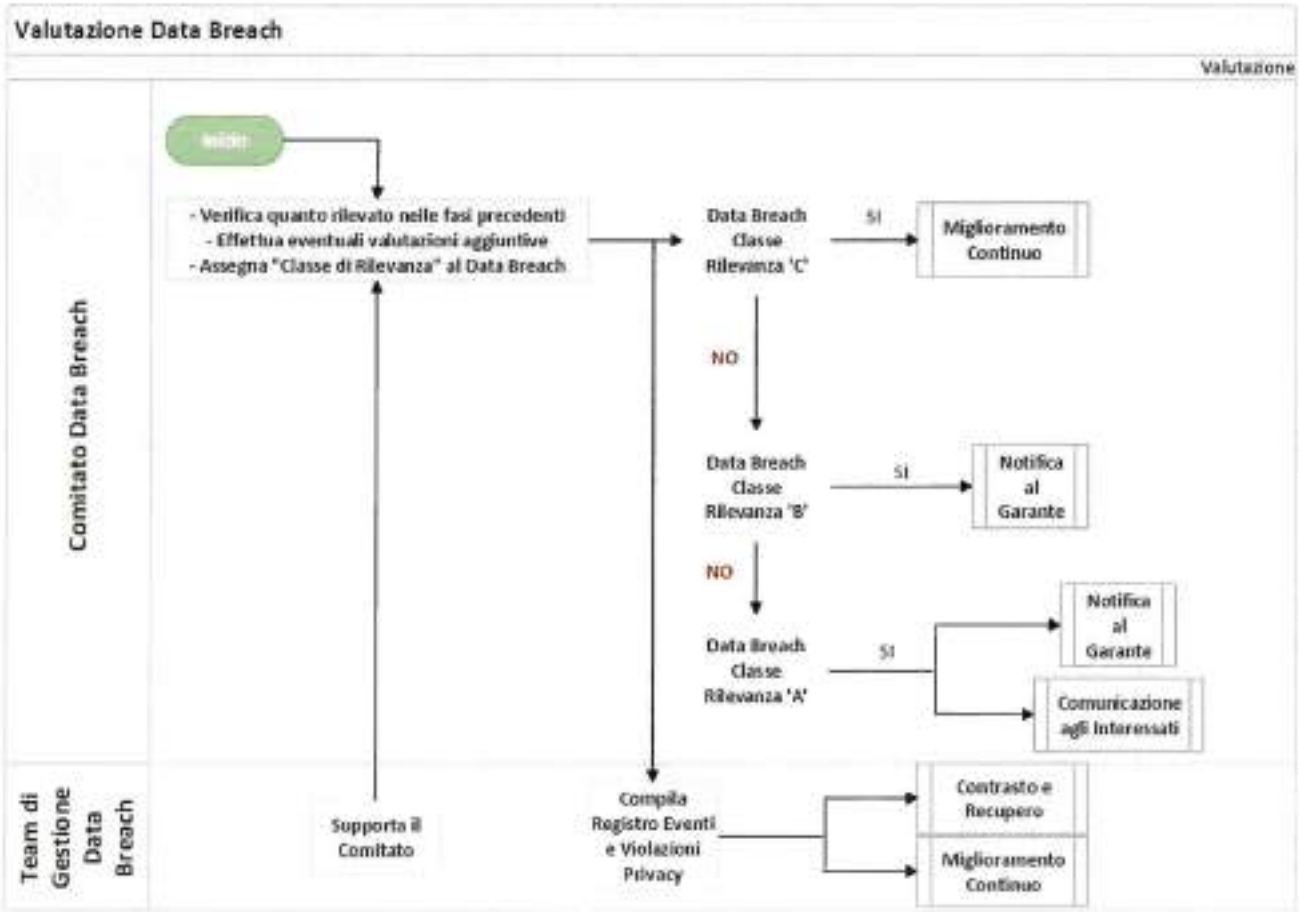

Figura 4 – Valutazione Data Breach

Il Comitato Data Breach, sulla base dei risultati della fase precedente, con il supporto del Team di Gestione Data Breach, svolge le seguenti attività:

- Verifica quanto rilevato nelle fasi precedenti;
- Effettua eventuali azioni aggiuntive;
- Assegna la "**Classe di Rilevanza**" al Data Breach.

La Classe di Rilevanza del Data Breach viene assegnata utilizzando la seguente scala valutativa:

- **Classe di Rilevanza A**: la violazione di dati personali in esame può comportare un elevato rischio per i diritti e le libertà delle persone fisiche;
- **Classe di Rilevanza B**: la violazione di dati personali in esame può comportare un rischio per i diritti e le libertà delle persone fisiche (la violazione può avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali);
- **Classe di Rilevanza C**: è improbabile che la violazione di dati personali in esame possa causare un rischio per i diritti e le libertà delle persone fisiche.

I seguenti esempi, non esaustivi, possono essere utili al Comitato Data Breach per stabilire se deve effettuare la notifica in diversi scenari di violazione dei dati personali, basati sulla linea guida di cui al [7]:

Esempio	Notifica all'autorità di controllo?	Comunicazione all'interessato?	Note/raccomandazioni
Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave USB viene rubata durante un'effrazione.	No.	No.	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave di cifratura univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati.	Sì, segnalare l'evento all'autorità di controllo se vi sono probabili conseguenze per le persone fisiche.	Sì, segnalare l'evento alle persone fisiche a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per tali persone è elevata.	
Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare del trattamento e accedere alle proprie registrazioni.	No.	No.	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. Il titolare del trattamento deve conservare adeguate registrazioni in merito.
Un titolare del trattamento	Sì, effettuare la	Sì, effettuare la	Se fosse stato disponibile un backup e i

Esempio	Notifica all'autorità di controllo?	Comunicazione all'interessato?	Note/raccomandazioni
subisce un attacco tramite *ransomware* che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa evidente che l'unica funzionalità dal *ransomware* era la cifratura dei dati e che non vi erano altri *malware* presenti nel sistema.	segnalazione all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	segnalazione alle persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	dati avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'autorità di controllo fosse venuta a conoscenza dell'incidente con altri mezzi, avrebbe potuto prendere in considerazione lo svolgimento di un'indagine al fine di valutare il rispetto dei requisiti di sicurezza più ampi di cui all'articolo 32.
Le cartelle cliniche di un ospedale sono indisponibili per un periodo di 30 ore a causa di un attacco informatico.	Sì, l'ospedale è tenuto a effettuare la notifica in quanto può verificarsi un rischio elevato per la salute e la tutela della vita privata dei pazienti.	Sì, informare le persone fisiche coinvolte.	
I dati personali di un gran numero di persone vengono inviati per errore a una mailing list sbagliata con più di 1 000 destinatari.	Sì, segnalare l'evento all'autorità di controllo.	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	

Tabella 2 - Esempi per la necessità di notifica del Data Breach

In sede di valutazione possono essere individuate ulteriori azioni di contrasto e recupero (cfr. par.2.3) o azioni di miglioramento (cfr. par. 2.7), in questo caso si applica quanto descritto nei paragrafi specifici.

Il Team di Gestione Data Breach aggiorna ed integra il "Registro Eventi e Violazioni Privacy" con le informazioni legate a tale fase.

60

2.5 Notifica al Garante

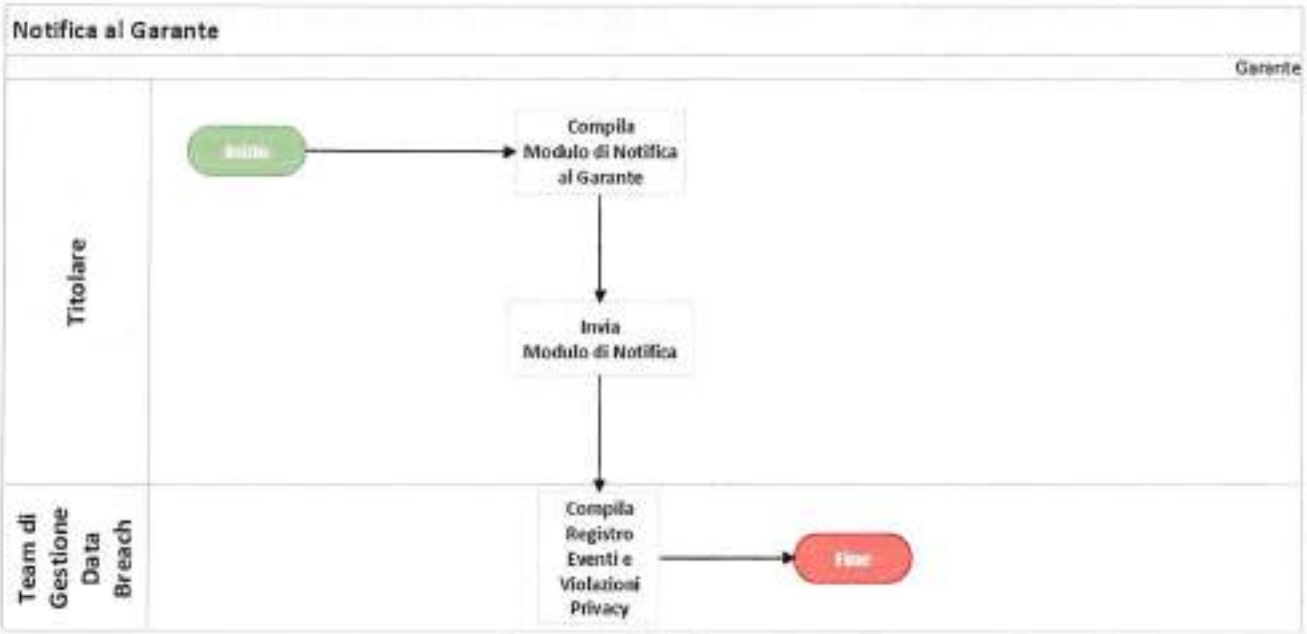

Figura 5 – Notifica al Garante

Se nella fase "Valutazione Data Breach" al Data Breach è stata assegnata la Classe di Rilevanza "B", oppure la Classe di Rilevanza "C", il Titolare deve inviare una Notifica al Garante sulla base del "Modulo di Notifica Data Breach al Garante" fornito in allegato (cfr. par. 3.2) **entro 72 ore dalla scoperta**, anche se i contorni della compromissione non sono chiari, fornendo le informazioni a disposizione.

Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo. Il DPO deve cooperare con il Garante e fungere da punto di contatto per quest'ultimo.

Il Team di Gestione Data Breach aggiorna ed integra il "Registro Eventi e Violazioni Privacy" con le informazioni legate a tale fase.

61

2.6 Comunicazione agli Interessati

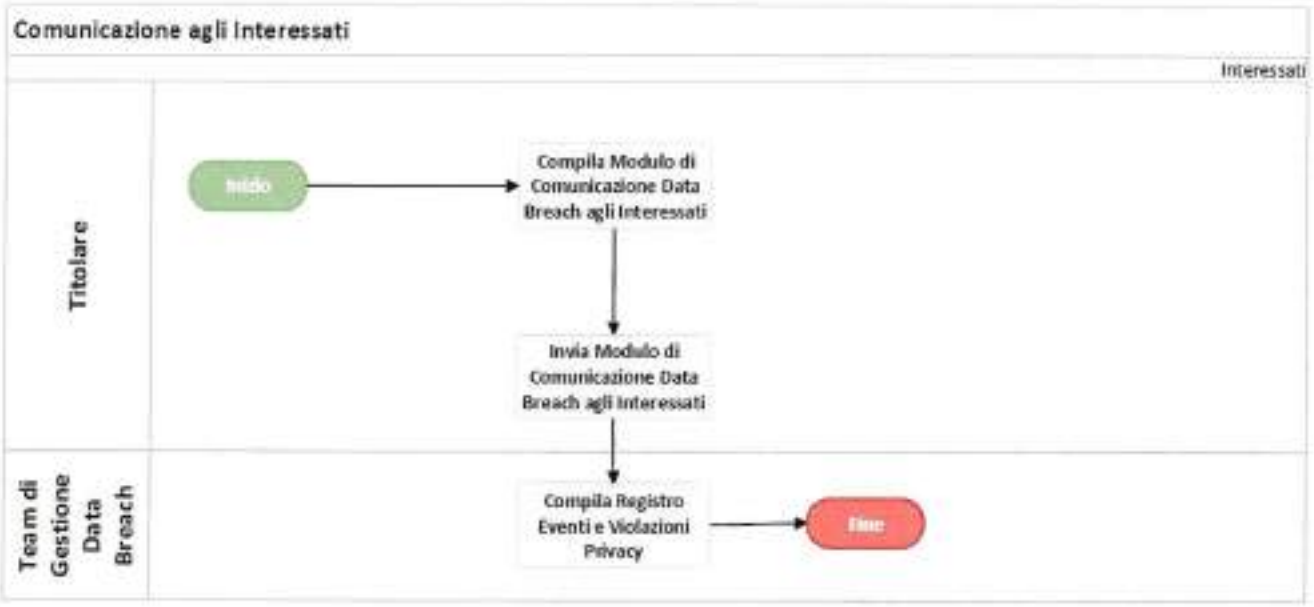

Figura 6 – Comunicazione agli Interessati

Se nella fase "Valutazione Data Breach" al Data Breach è stata assegnata la Classe di Rilevanza "C", oltre ad inviare la notifica al Garante (par. 2.5), il Titolare deve comunicare la violazione dei dati personali a tutti gli Interessati coinvolti, utilizzando i canali più idonei.

Il DPO deve fungere da punto di contatto per gli Interessati.

La comunicazione agli Interessati, secondo quanto previsto dal paragrafo n. 3 dell'art. 34 del GDPR, non è richiesta se è soddisfatta una delle seguenti condizioni:

- Il Titolare del trattamento ha messo 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;
- Il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- Detta comunicazione richiederebbe sforzi sproporzionati.

Nell'ultimo caso, si procede invece ad una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia.

La comunicazione deve essere effettuata utilizzando il "Modulo di comunicazione Data Breach agli Interessati" fornito in allegato (cfr. par. 3.3).

62

Il Team di Gestione Data Breach aggiorna ed integra il "Registro Eventi e Violazioni Privacy" con le informazioni legate a tale fase.

2.7 Miglioramento Continuo

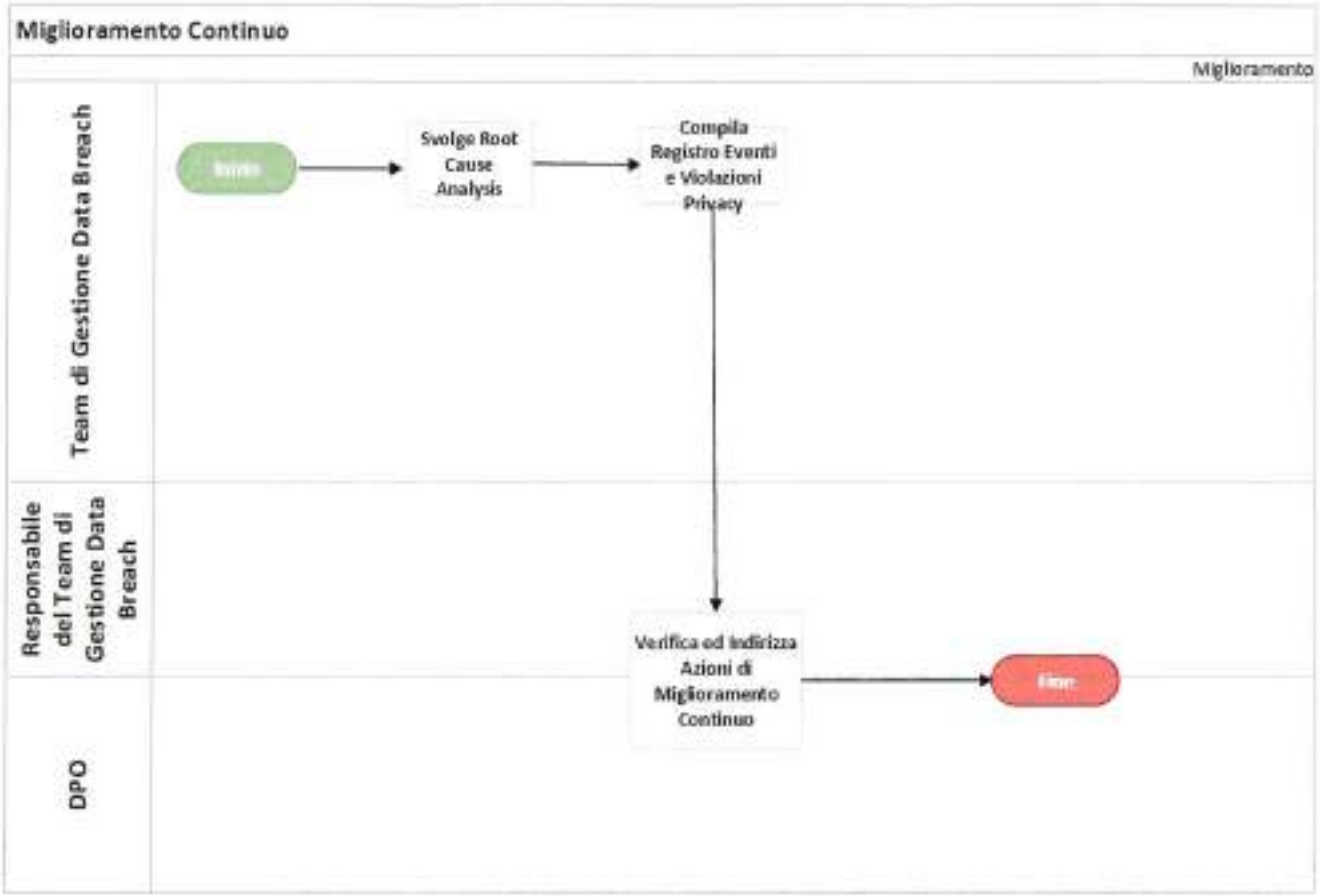

Figura 7 – Miglioramento Continuo

La gestione del Data Breach non costituisce unicamente un insieme di attività di tipo reattivo rispetto ad eventi potenzialmente dannosi, ma anche di tipo proattivo. Ciò comporta che gli esiti della gestione di Data Breach occorsi nel passato rappresentano la base per indirizzare nella maniera più efficace possibile il trattamento di violazioni future.

A valle della risoluzione della violazione dei dati personali, il Team di Gestione Data Breach conduce una "root cause analysis" della violazione, ovvero un'analisi svolta a posteriori per individuare i fattori che ne hanno determinato l'accadimento.

La root cause analysis consiste nell'arricchimento di quanto riportato nel "Registro Eventi e Violazioni Privacy" (sezione specifica per questa fase) con il seguente insieme di informazioni che deriva dalla considerazione di più fattori:

- Numero totale di segnalazioni/rilevazioni strumentali riconducibili all'evento occorso:
    - Comunicazioni da più referenti della stessa rispondenza di violazione anche in tempi diversi;
    - Anomalie riscontrate da altri strumenti di monitoraggio, da considerare in aggiunta alla rilevazione dell'evento;
- Momento esatto dell'accadimento della violazione, ovvero se riconducibile ad altra evidenza antecedente rispetto alla segnalazione/rilevazione;
- Eventuale vulnerabilità sfruttata;
- Verifica della presenza dei controlli preventivi necessari ed efficacia di quelli effettivamente implementati:
    - Analisi log;
    - Opportuna configurazione apparati di protezione;
    - Hardening dei sistemi;
    - Patching dei sistemi;
    - Attuazione corretta delle istruzioni operative;
- Dettaglio ex-post della tipologia di dati coinvolti e dei sistemi/infrastrutture tecnologiche impattati;
- Eventuali azioni inibitorie alle attività di contrasto o alla loro tempestività:
    - Indisponibilità temporanea o permanente delle risorse tecnologiche per il contenimento;
    - Impedimenti di natura organizzativa;
- Indicazione della codifica di eventuali eventi pregressi con analoghe caratteristiche (e.g. data/ora accadimento, sistema/piattaforma target).

Il DPO ed il Responsabile Team di Gestione Data Breach, verificate le risultanze della attività si "root cause analysis", indirizzano le azioni di natura correttiva/evolutiva atte a:

- Ottimizzare e velocizzare la gestione di occorrenze di eventi e violazioni di dati personali future;
- Migliorare la gestione dei Data Breach;
- Affinare i sistemi di rilevazione e segnalazione eventi;
- Migliorare i processi atti a proteggere i dati personali (e.g. nuovi controlli correttivi e/o preventivi, ridefinizione processi e procedure, ridefinizione istruzioni operative, definizione piani di formazione).

64

3 Allegati

3.1 Allegato 1: Modulo di Segnalazione Data Breach

Modulo
Segnalazione Data E

3.2 Allegato 2: Modulo di Notifica Data Breach al Garante

Modulo di Notifica
Data Breach al Gara

3.3 Allegato 3: Modulo di Comunicazione Data Breach agli Interessati

Modulo
Comunicazione Dati

3.4 Allegato 4: Modulo di Registro Eventi e Violazioni Privacy

Registro Eventi e
Violazioni Privacy.xls

65