Procedura
per la Gestione delle
Violazioni di Dati Personali
(*Data Breach*)

ai sensi degli artt.33-34 del Regolamento UE 2016/679

Procedura	versione	data di redazione	delibera di adozione	modifiche
PR_DB_01_Procedura_data_breach				

Sommario

1 Introduzione

La normativa vigente in materia di Protezione dei Dati Personali, costituita dal Regolamento UE 679/2016 – Regolamento sulla Protezione dei Dati (di seguito anche il "Regolamento") e dal D.Lgs. 196/2003 – Codice in materia di Protezione dei Dati Personali (di seguito anche il "Codice"), così come modificato dal D.Lgs. 101/2018, ha l'obiettivo di proteggere i dati personali degli interessati al fine di evitare che un uso non corretto delle informazioni possa danneggiare o ledere le libertà fondamentali e la dignità degli interessati.
Le tipologie di dati personali trattati dall'Azienda Sanitaria Locale della Provincia di Foggia (d'ora in avanti anche "ASL FOGGIA" o "Azienda") sono costituiti principalmente sia da dati personali (ad esempio dati anagrafici, recapiti, identificativi di tessera sanitaria, codici fiscali, ecc…) che da dati appartenenti a categorie particolari, quali i dati relativi alla salute degli assistiti.
L'Azienda predispone il presente documento nell'ambito del proprio sistema organizzativo a tutela dei dati personali degli interessati.

2 Scopo

Il presente documento descrive le modalità operative adottate dall'ASL FOGGIA, per poter rispettare quanto previsto dagli artt. 33 e 34 del Regolamento UE 679/2016: in particolare viene definito un flusso di attività da attivarsi nel caso in cui dovesse manifestarsi un evento di violazione dei dati personali rispetto a quanto definito esplicitamente dalla normativa vigente o dalle regolamentazioni interne dell'Azienda.

L'obiettivo del presente documento è di fornire una descrizione generale del processo di gestione delle Violazioni di Dati Personali e delle relative indicazioni operative immediate per poter procedere con la rilevazione, la valutazione ed il contenimento della violazione; viene inoltre valutata la necessità di dover procedere con la comunicazione all'Autorità Garante per la Protezione dei Dati Personali ed eventualmente all'interessato.

3 Campo di Applicazione

Per Violazione di Dati Personali (cd. "*Data Breach*") si intende 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.

La presente procedura operativa si applica, nello specifico, a tutto il personale dell'ASL FOGGIA che tratta a qualsiasi titolo e in qualsiasi modalità (digitale, cartacea, etc.) dati personali e, ove applicabile, alle terze Parti che operano per conto dell'Azienda.

Il presente documento determina il processo di gestione delle violazioni di dati personali che possono accadere al manifestarsi di eventi come i seguenti (a titolo esemplificativo e non esaustivo):

- Accesso non autorizzato ai dati personali
- Azioni accidentali o deliberate da parte dei soggetti autorizzati al trattamento
- Invio dei dati a un destinatario errato
- Perdita o furto di dispositivi di memoria o computer portatili che contengono dati personali
- Alterazione non autorizzata dei dati personali
- Perdita della disponibilità dei dati personali

4 Definizioni

Le seguenti definizioni sono di utilità per poter dare le risposte opportune nell'ambito del questionario in base all'art. 4 del Regolamento:

«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;

«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

«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;

«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

«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;

«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

«destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

«consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

«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;

«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

«dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

«banca di dati»: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

«evento sulla sicurezza delle informazioni»: occorrenza identificata di uno stato di un sistema, servizio o della rete che indichi una possibile violazione di una policy sulla sicurezza delle informazioni (Information Security Policy) o il fallimento di controlli, o una situazione precedentemente sconosciuta che può essere rilevante a fini di sicurezza

«incidente sulla sicurezza delle informazioni»: evento singolo o serie di eventi sulla sicurezza delle informazioni indesiderati o imprevisti che hanno una significativa probabilità di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni

«DPO»: *Data Protection Officer* o Responsabile della Protezione Dati

5 Normativa di Rifermento

La procedura contenuta nel presente documento descrive i passi da seguire nel caso si verifichi un evento di violazione di dati personali, in conformità con quanto stabilito dagli artt.33-34 del Regolamento UE 2016/679 (GDPR) che stabiliscono i seguenti obblighi in capo all'ASL FOGGIA, in qualità di Titolare del trattamento:

- Obbligo di notifica all'Autorità Garante "senza ingiustificato ritardo" e, ove possibile, entro 72 ore (art. 33 del GDPR).
- Obbligo di comunicazione agli interessati quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 34 del GDPR)

In particolare:

5.1 Articolo 33 – Reg UE 679/2016 Notifica di una violazione di dati

1. In caso di **violazione dei dati personali**, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente, a norma dell'articolo 33 del GDPR, 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.

2. Il Responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1, effettuata tramite procedura telematica sul sito web dell'Autorità Garante per la protezione dei dati:

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

b) comunica il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrive le probabili conseguenze della violazione dei dati personali;

d) descrive le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il Titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente al Garante di verificare il rispetto del presente articolo.

5.2 Articolo 34 – Reg UE 679/2016 – Comunicazione di una violazione di dati

1. Quando la violazione dei dati personali è suscettibile di presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33 del GDPR, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) 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;

b) 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;

c) 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.

4. Nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante Privacy può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

6 Team di Risposta alle Violazioni ed elementi di valutazione

6.1 Team di Risposta alle Violazioni *(Data Breach Response Team)*

Il Team di Risposta alle Violazioni (*data breach*) è una entità multidisciplinare composta da soggetti che presentano conoscenze e competenze tali da assumersi la responsabilità per valutare e porre in essere le misure di contenimento le conseguenze negative della violazione.

La composizione del Team è costituita in maniera fissa da referenti delle Strutture Organizzative direttamente coinvolte nella gestione della Protezione dei Dati Personali e opzionalmente, su richiesta da parte dei componenti di base del Team, da ulteriori referenti. Il Team è composto dai Direttori/Responsabili delle Macro-strutture di seguito elencati o da loro delegati.

Team di Risposta alle Violazioni		
Funzione interna	**Competenza**	**Partecipazione**
S.S. Sistemi Informativi e Telecomunicazioni	Conoscenza dell'infrastruttura di rete, delle misure di sicurezza idonee adottate e delle infrastrutture tecnico-applicative impiegate per il trattamento dei dati	Componente di base
RTD	Responsabile per la Transizione al Digitale	Componente di base
Responsabile Sicurezza informatica	Responsabile della Sicurezza informatica aziendale	Componente di base
Responsabile della conservazione	Responsabile della conservazione	Componente di base
Responsabile della gestione documentale	Responsabile della gestione documentale	Componente di base
Data Protection Officer	Responsabile per la Protezione dei Dati Personali	Componente di base
Ingegneria Clinica	Conoscenza approfondita del patrimonio tecnologico medicale e delle tecnologie biomediche impiegate per il trattamento dei dati	Componente di base

Direzione Generale/Direzione Amministrativa/Direzione Sanitaria	Organi di vertice cui competono le decisioni finali	Componenti di base
Ufficio Privacy	A conoscenza del quadro normativo nazionale ed europeo. Struttura competente per il mantenimento della *compliance* alle normative privacy nazionali ed europee	Componente di base
Area Formazione	Programmazione delle attività formative dedicate al personale aziendale	Componente di base
Area Gestione Patrimonio	Struttura competente alla stipulazione di contratti e procedure negoziate	Componente di base
Medicina Legale e Gestione Rischio Clinico	Ha la funzione di attuare le scelte aziendali di gestione del rischio clinico con azioni di prevenzione o di contenimento e di eliminazione dei fattori di rischio o errore insiti nelle attività erogate di diagnosi, cura e riabilitazione. Assicura le attività specialistiche medico legali della ASL.	Componente di base
Programmazione aziendale	Struttura competente alla programmazione delle attività e di valutazione dei servizi erogati dalla ASL	Opzionale – su richiesta
Direttore/Responsabile della Struttura organizzativa in cui si è verificato l'evento	Possono fornire ulteriori informazioni e supporto per un efficace risposta al data breach	In base all'Area organizzativa in cui si verifica l'evento

Il Responsabile dell' Ufficio Privacy/DPO è il soggetto che coordina il Team di Risposta alle Violazioni.

Il Team deve assicurare un'adeguata tempestività nella risposta alle violazioni, oltre a fornire tutte le risorse necessarie per il contrasto dell'evento e la preparazione necessaria per la risposta.

Se necessario, i membri del team possono farsi aiutare da team esterni, come ad esempio le Terze parti che si occupano di sicurezza informatica, società di analisi forense dei dati etc.

Opzionalmente, in base alle necessità, il Responsabile può integrare ulteriore personale nel Team se utile al contrasto di una specifica violazione.

Il Team di Risposta alle Violazioni (*Data Breach Response Team*) deve essere preparato alla risposta di presunte o accertate violazioni e reperibile. A tal fine, è necessario avere a disposizione una lista dei numeri di contatto di ogni membro facente parte del Team e l'autorizzazione per queste persone ad essere reperibili.

6.1.1 Compiti del Team

A valle della segnalazione della violazione, il Team dovrà:

- **Validare/rispondere alla violazione**
- **Predisporre un'appropriata e imparziale investigazione, documentandola correttamente**
- **Identificare gli eventuali asset da bonificare e tenere traccia delle misure da porre in essere per risolvere le vulnerabilità**
- **Coordinarsi con le Autorità se necessario**
- **Coordinarsi per la comunicazione verso l'interno e verso l'esterno**

- **Preoccuparsi di rispettare gli obblighi di notifica e comunicazione**
- **Analizzare ogni incidente e tenere traccia della Violazione nell'apposito registro**
- **Rendicontare alla Direzione Strategica**

6.2 Informazioni preliminari per la valutazione delle violazioni

Nell'ambito delle valutazioni relative alla gravità (*severity*) delle violazioni dovranno essere tenuti in considerazione i seguenti fattori di rischio per i diritti e le libertà dei soggetti interessati:

a) Tipo di violazione
b) Natura, carattere sensibile e volume dei dati personali
c) Facilità di identificazione delle persone fisiche
d) Gravità delle conseguenze per le persone fisiche
e) Caratteristiche particolari dell'interessato
f) Numero di persone fisiche interessate
g) Contesto di riferimento

In particolare, per tipo di violazione si intende:

- **Violazione della Riservatezza** (cd. *Confidentiality Breach*) accesso accidentale o illecito ai dati personali o divulgazione degli stessi;
- **Violazione della Disponibilità** (cd *Availibility Breach*) perdita o distruzione accidentale o illecita del dato personale;
- **Violazione dell'Integrità** (cd *Integrity Breach*) quando vi è una modifica accidentale o non autorizzata del dato personale.

7 Descrizione del Processo

Il processo contenuto nel presente documento descrive i passi da seguire nel caso si verifichi un evento di Violazione del Dati Personali in conformità con quanto stabilito dagli Artt.33-34 del Regolamento UE 2016/679.

Il processo si articola nelle seguenti fasi:

- **Rilevazione di una Violazione di Dati Personali**
- **Gestione della Violazione (Valutazione e Decisione)**
- **Risposta all'evento**
- **Notifica all'Autorità Garante**
- **Comunicazione agli Interessati**
- **Documentazione della Violazione**

7.1 Rilevazione della Violazione di Dati Personali

Le segnalazioni di eventi che portano a violazioni sui dati personali possono avvenire tramite canali interni ed esterni:

1) **CANALI INTERNI**

Le segnalazioni di eventi anomali possono provenire internamente da:

- **Personale dell'ASL FOGGIA**: Le violazioni di dati personali sono gestite dal Team come sopra riportato. In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.

- **Nel caso in cui un dipendente**, in qualità di Soggetto Autorizzato al Trattamento dei Dati, si accorga di una concreta, potenziale o sospetta violazione dei dati personali, deve immediatamente informare il proprio superiore gerarchico (Soggetto Autorizzato al Trattamento con Delega) della possibile violazione. Quest'ultimo dovrà quindi informare il superiore gerarchico ed il Responsabile Protezione Dati (DPO) mediante la compilazione della sezione A dell'allegato "PR-MOD-01 – Segnalazione_valutazione della Violazione" da trasmettere all'indirizzo email rpd@aslfg.it.

- **S.S. Sistemi informativi e Telecomunicazioni**: mediante opportuni strumenti di monitoraggio di eventi di natura Software e ICT: tale monitoraggio include l'insieme delle attività di controllo finalizzate al rilevamento degli eventi tracciati dai sistemi informatici e dai sistemi di security ICT aziendale. Tali eventi relativi ai sistemi ICT sono sotto responsabilità e conseguentemente monitorati e gestiti dalla S.S. e dagli Amministratori di Sistema opportunamente incaricati. In caso di rilievo di concreta, sospetta e/o avvenuta violazione dei dati personali relativi ai sistemi ICT aziendali, l'Amministratore di Sistema o il Soggetto Autorizzato al Trattamento dei Dati Personali autorizzato al monitoraggio degli eventi informatici deve immediatamente informare il Responsabile Ufficio Privacy ed il Responsabile Protezione Dati (DPO) mediante la compilazione della sezione A dell'allegato "PR-MOD-01 – Segnalazione_valutazione della Violazione" da trasmettere all'indirizzo email rpd@aslfg.it.

2) **CANALI ESTERNI**

Le segnalazioni di eventi anomali possono pervenire anche dall'esterno:

- **Segnalazione dall'interessato**: l'interessato del trattamento (assistito, utente, consulente, etc..) può effettuare una segnalazione anche in caso di semplice sospetto che i propri dati personali siano stati utilizzati in maniera fraudolenta da terzi o in generale che siano stati oggetto di violazione. In questi casi, l'interessato dovrà rivolgersi al DPO per la verifica di eventuali violazioni secondo quanto disposto dall'informativa Privacy disponibile sul sito internet istituzionale;

- **Segnalazione dal Responsabile del Trattamento**: il Responsabile del Trattamento (terza parte che tratta dati per conto dell'ASL FOGGIA), in caso si accorga di una concreta, potenziale o sospetta violazione dei dati personali, deve immediatamente informare il referente dell'ASL FOGGIA (Soggetto Autorizzato al Trattamento con Delega – SATD) della possibile violazione; il Responsabile è tenuto ad assistere il SATD nell'informare l'Ufficio Privacy ed il Responsabile Protezione Dati (DPO) mediante la compilazione della sezione A dell'allegato "PR-MOD-01 – Segnalazione_valutazione della Violazione" da trasmettere all'indirizzo email rpd@aslfg.it.

7.2 Gestione della violazione (Valutazione e Decisione)

La gestione di una violazione dei dati personali è stata standardizzata in un processo suddiviso nelle seguenti quattro fasi:

1) Analisi preliminare delle segnalazioni.
2) *Risk Assessment* e individuazione misure per il contenimento della violazione
3) Notifica all'Autorità Garante.
4) Comunicazione agli interessati

7.2.1 Analisi preliminare delle segnalazioni

La Struttura incaricata della valutazione delle segnalazioni di Violazioni di Dati Personali è l'Ufficio Privacy che grazie al team multidisciplinare effettuerà una analisi preliminare sulle informazioni relative alla presunta violazione, raccolte attraverso l'apposito modulo di Segnalazione (allegato "PR-MOD-01 – Segnalazione_valutazione della Violazione"), avendo in tal modo un quadro strutturato sull'anomalia segnalata.
A seguito di ricezione della segnalazione, il Team di risposta alle violazioni, con il supporto del Responsabile della Protezione Dati (DPO), effettua una valutazione preliminare (sezione B dell'allegato) riguardante la possibile violazione occorsa, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di Violazione (*Data Breach*) e se sia necessaria un'indagine più approfondita dell'accaduto.
Nel caso in cui l'evento venga accertato come "falso positivo", la procedura di verifica viene archiviata su disposizione del Direttore Generale (sezione C dell'allegato) e l'evento viene comunque inserito all'interno del Registro delle Violazioni (allegato "PR-REG_DB_01- Registro data breach" gestito dall'Ufficio Privacy.

NB: al fine di una migliore valutazione in termini di impatto per i soggetti interessati, le valutazioni dovranno tenere conto di tali 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 e pazienti;**
d) **che il trattamento riguardi una notevole quantità di dati personali;**
e) **che il trattamento riguardi un vasto numero di interessati.**

Nel caso in cui si individuasse una possibile violazione di dati contenuti in un sistema informatico, il Responsabile Ufficio Privacy, in qualità di Coordinatore del Team di risposta alle violazioni, inoltra la segnalazione, oltre che al Responsabile Protezione Dati, anche all'Amministratore di Sistema e/o Responsabile del trattamento (fornitore ICT) di competenza per avviare l'istruttoria e le valutazioni di merito.
Detta valutazione preliminare viene effettuata attraverso l'esame delle informazioni riportate nell'Allegato "PR-MOD-01 – Segnalazione_valutazione della Violazione", quali:
• la data di scoperta della violazione (tempestività);
• Il soggetto che è venuto a conoscenza della violazione;
• la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
• le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
• la descrizione di eventuali azioni già poste in essere.

Di seguito i criteri di valutazione della gravità del *data breach* presenti nel modulo "PR-MOD-01 – Segnalazione_valutazione della Violazione":

1 - **Rischio Basso**: gli interessati coinvolti dal trattamento non saranno affetti da inconvenienti oppure possono incontrare alcuni inconvenienti che possono superare senza alcun problema (es. perdita di tempo per ripetere formalità, etc.);
2 – **Rischio Medio**: gli interessati coinvolti dal trattamento possono incontrare disagi significativi che però possono superare nonostante alcune difficoltà (es. interruzione temporanea del servizio fino a 8 ore);
3 – **Rischio Alto**: gli interessati coinvolti dal trattamento possono avere conseguenze significative che dovrebbero essere in grado di superare seppure con gravi difficoltà (es. interruzione temporanea del servizio oltre le 24 ore);
4 – **Rischio Elevato**: gli interessati coinvolti dal trattamento possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (es.: Interruzione del servizio oltre le 48 ore, impossibilità o perdita della possibilità di accesso ai servizi, mancato rispetto dei diritti dell'interessato – es.: diritto alla salute)
0 – Nessun rischio: Nel caso di nessun rischio, non si è verificato un incidente di sicurezza che ha comportato la perdita di riservatezza, integrità o disponibilità di dati e di conseguenza non c'è stata una violazione dei dati personali.

- ✓ **Nel caso di livello di rischio basso o medio, la violazione non rientra tra quelle soggette a comunicazione al Garante Privacy;**
- ✓ **Nel caso di livello di rischio alto, la violazione deve essere comunicata al Garante Privacy ma non all'interessato;**
- ✓ **Nel caso di livello di rischio elevato, la violazione deve essere comunicata sia al Garante Privacy che all'interessato;**
- ✓ **Nel caso di nessun rischio, l'evento è classificato come falso positivo nel registro interno dei data breach;**

7.2.1.1 Azioni di Contenimento

Alcune *best practices* da attuare come primo approccio alle violazioni sono quelle elencate di seguito in presenza di data breach su sistemi informatizzati.

1. **Contenere i dispositivi infettati impostandoli *off-line***
2. **Censire i dispositivi che sono stati violati**
3. **Individuare quali vulnerabilità sono state sfruttate per violare i dispositivi/sistemi ed eventualmente gli apparati di comunicazione**
4. **Raccogliere evidenze per il Garante in modo tale da dimostrare quali misure siano state impiegate e quali azioni siano state attuate durante il *data breach***
5. **Ripristinare i dispositivi/sistemi e le reti**
6. **Integrare le informazioni raccolte per individuare nuove misure al fine di stabilire un nuovo Piano per la sicurezza per far sì che l'incidente non avvenga in futuro.**

7.2.2 Risk Assessment e individuazione delle misure

A termine della fase di valutazione preliminare, nel caso si stabilisca che una possibile violazione è effettivamente avvenuta, il Responsabile Protezione Dati (DPO)/il Responsabile Ufficio Privacy, stabiliscono congiuntamente:

- le **opportune misure correttive e di protezione che possano limitare i danni** che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso… *ecc.*);
- le **modalità e le tempistiche** di suddette misure, individuando gli attori e i compiti per limitare la violazione;
- se la violazione ricade nei casi in cui è necessario **notificare** all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se l'entità della violazione necessiti di **comunicare il *data breach* agli interessati** (ove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità Garante per la protezione dei dati e di comunicazione agli interessati, il Responsabile delle Protezione dati/il Responsabile Ufficio Privacy valuteranno la gravità della violazione utilizzando il modello in allegato "PR-MOD-01 – Segnalazione_valutazione della Violazione".

7.2.3 Notifica all'Autorità Garante competente

Se a seguito delle valutazioni preliminari e del *risk assessment* effettuato nel rispetto della presente procedura, è stata verificata la necessità di effettuare la notifica della violazione dei dati, secondo quanto prescritto dal Regolamento UE 2016/679, la Direzione Generale, con il supporto dell'Ufficio Privacy, provvede alla notifica all'Autorità Garante per la protezione dei dati, senza ingiustificato ritardo e, ove possibile **entro 72 ore** dal momento in cui ne è venuto a conoscenza.

La notifica deve essere inviata attraverso l'apposita procedura telematica prevista dal Garante all'indirizzo https://servizi.gpdp.it, giusto Provvedimento del Garante n. 209 del 27 maggio 2021 -

Procedura telematica per la notifica di violazioni di dati personali (*data breach*). In particolare, nella stessa pagina web è disponibile:

- un modello facsimile (allegato "**PR-MOD-03_ Fac-simile Notifica al Garante**"), da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante;
- un apposito strumento di autovalutazione (*self assessment*) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza (disponibile all'indirizzo https://servizi.gpdp.it/databreach/s/self-assessment);
- le istruzioni per l'utilizzo della procedura telematica per la notifica delle violazioni dei dati personali.

Il Titolare, qualora necessario, comunica la violazione di dati ad altre Autorità competenti (Autorità giudiziaria, CSIRT etc.).

7.2.4 Comunicazione agli interessati

Ove a seguito delle valutazioni preliminari e del *risk assessment* effettuato nel rispetto della presente procedura, venga rilevata la necessità di effettuare la comunicazione della violazione dei dati anche ai diretti interessati, in presenza di un **rischio elevato per i diritti e le libertà delle persone fisiche**, la Direzione Generale, per il tramite dell' Ufficio Privacy, provvederà alla comunicazione all'Interessato senza ingiustificato ritardo utilizzando il modello in allegato "**PR-MOD-02 - Comunicazione Interessato**".

Il contenuto della comunicazione prevede:

- il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Il messaggio dovrà essere comunicato in maniera diretta e trasparente. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, è possibile utilizzare una comunicazione pubblica (ad es. tramite il sito web istituzionale), che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

La comunicazione all'interessato di cui al paragrafo 1 del l'art. 34 del Regolamento UE 2016/679 deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del Regolamento UE 2016/679.

3.Nei seguenti casi non è richiesta la comunicazione all'interessato:

a) l'Azienda 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;
b) l'Azienda ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

7.3 Documentazione della violazione

Qualsiasi tipo di violazione di dati personali è documentato dall'Ufficio Privacy con il supporto dei componenti del Team di risposta alle violazioni, ai sensi dell'art. 33 c.5 del Regolamento UE 2016/679.

Il Responsabile dell'Ufficio Privacy provvede alla tenuta e diligente custodia dell'apposito Registro delle Violazioni (allegato "PR-REG_DB_01- Registro data breach"), in cui sono riportate almeno le seguenti informazioni:

Rilevazione data breach

- ✓ data della violazione
- ✓ descrizione sintetica della violazione
- ✓ tipo violazione (riservatezza-integrità-disponibilità)
- ✓ link al modulo "PR-MOD-01 - Segnalazione della Violazione"
- ✓ link al modulo "PR-MOD-02 - Comunicazione Interessato"
- ✓ attività di trattamento di dati personali coinvolti

Archiviazione

- ✓ data archiviazione evento

Notifica Garante (se presente)

- ✓ data della notifica al Garante
- ✓ tipo notifica (completa o preliminare)
- ✓ rif. protocollo/fasc/pin

Comunicazione Interessati (se presente)

- ✓ data della comunicazione
- ✓ modalità di comunicazione
- ✓ rif. protocollo comunicazione

Provvedimento Garante (se presente)

- ✓ link a provvedimento dell'Autorità Garante

Note

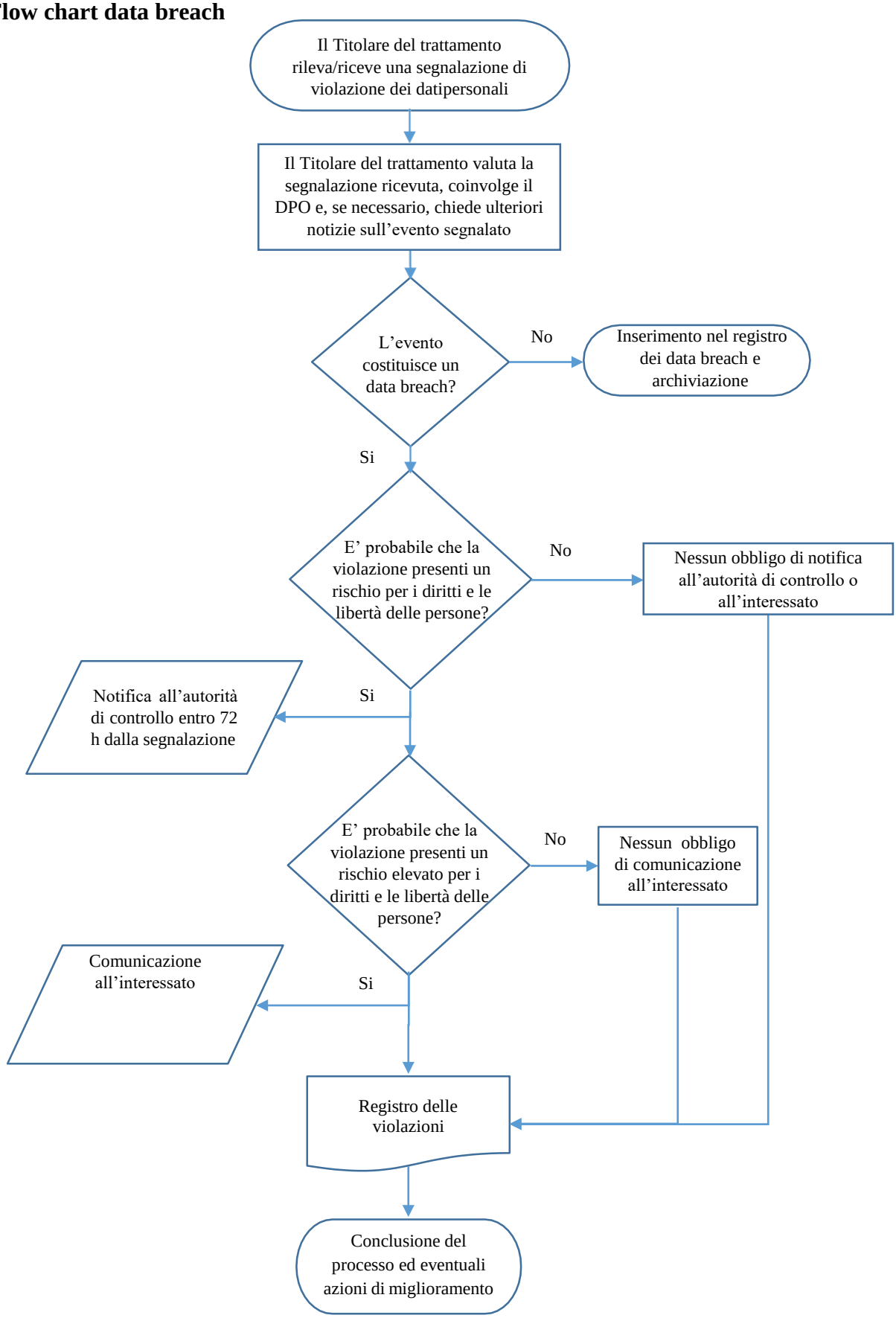
- ✓ informazioni aggiuntive

7.4 Analisi post violazione

Dopo aver posto in essere i precedenti adempimenti, è necessaria la raccolta finale delle evidenze, l'analisi delle informazioni giunte sul contesto di violazione osservato, e la valutazione delle stesse al fine di effettuare

un'analisi post-incidente, per verificare l'efficacia e l'efficienza delle azioni intraprese durante la gestione dell'evento ed identificare possibili aree di miglioramento che svilupperanno ulteriormente l'efficacia del piano di gestione delle violazioni.

8 Flow chart data breach



9 Casistiche

I seguenti esempi, non esaustivi, possono essere utili al Team di risposta alle violazioni, per stabilire se deve essere effettuata la notifica all'Autorità Garante per la protezione dei dati, in diversi scenari di violazione dei dati personali:

Esempio	Notifica al Garante?	Comunicazione all'interessato?	Note
Il 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
Il Titolare del trattamento gestisce un servizio on-line. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati.	Sì, segnalare l'evento al Garante se vi sono probabili conseguenze negative per le persone fisiche.	Sì, segnalare l'evento alle persone fisiche a seconda della natura dei dati personali interessati e della gravità delle conseguenze per tali persone	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 al Garante.
Una breve interruzione di corrente di alcuni minuti presso la sede di un titolare del trattamento impedisce agli utenti di contattare gli Uffici	No	No	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5 del GDPR. Il titolare del trattamento deve conservare adeguate registrazioni in merito.

Il Titolare del trattamento subisce un attacco tramite ransomware che provoca la cifratura di tutti i dati, non più accessibili. Sono disponibili i backup e i dati possono essere ripristinati in tempi rapidi.	No	No	Se fosse stato disponibile un backup e i dati avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione al Garante o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora il Garante fosse venuto 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'art.32 del GDPR.
Il Titolare del trattamento subisce un attacco tramite ransomware che provoca la cifratura di tutti i dati, non più accessibili. Non sono disponibili i backup e i dati non possono essere ripristinati in tempi rapidi.	Sì, effettuare la segnalazione al Garante.	Si, effettuare la comunicazione all'interessato.	Se fosse stato disponibile un backup e i dati avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione al Garante o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora il Garante fosse venuto 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'art.32 del GDPR.
Una cartella clinica cartacea di un paziente è stata smarrita con successiva denuncia effettuata dal titolare.	Sì, effettuare la segnalazione al Garante.	Si, effettuare la comunicazione all'interessato.	
Un referto medico è consegnato a persona diversa dal destinatario per errore umano	Sì, effettuare la segnalazione al Garante.	Si, effettuare la comunicazione all'interessato.	
Una determina contenente dati personali e relativi allo stato di salute di un assistito è disponibile in Albo pretorio on-line e/o Amministrazione Trasparente	Sì, effettuare la segnalazione al Garante.	Si, effettuare la comunicazione all'interessato.	

10 Diffusione della procedura

La presente procedura è divulgata in modo capillare e pubblicata sul sito internet istituzionale della ASL FOGGIA nell'apposita sezione "Privacy".

11 Allegati

- **PR-MOD-01 – Segnalazione_Valutazione della Violazione**
- **PR-MOD-02 - Comunicazione Interessato**
- **PR-MOD-03_ Fac-simile Notifica al Garante**
- **PR-REG_DB_01- Registro data breach**