Regione Abruzzo

Procedura per la Gestione delle Violazioni di Dati Personali - Data Breach

della ASL Teramo

in base a quanto previsto dagli

Artt. 33 e 34 del Regolamento UE 2016/679 (GDPR)

Redazione	Verifica	Parere favorevole	Approvazione
R.T.I.	UOSD Segreteria di Direzione	D.P.O.	Titolare

Sommario

1 Introduzione

La normativa vigente in materia di Protezione dei Dati Personali, costituita dal Regolamento UE 2016/679 – 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") 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. Considerato il contesto operativo dell'Azienda Sanitaria, tali problematiche sono di notevole rilevanza.
Le tipologie di dati personali trattati dall'Azienda Sanitaria sono costituite principalmente sia da dati personali (ad esempio dati anagrafici, recapiti, identificativi di tessera sanitaria, codici fiscali, ecc…) sia da "particolari categorie di dati personali" quali i dati relativi alla salute.
La ASL n. 04 di Teramo (di seguito anche la "ASL") 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 dalla ASL di Teramo, per poter rispettare quanto previsto dagli artt. 33 e 34 del Regolamento UE 2016/679 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 Sanitaria.

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.*

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 in base all'art. 4 del Regolamento sono di utilità per poter comprendere al meglio quanto descritto nella presente procedura:

«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 Riferimento

Il processo contenuto nel presente documento descrive le attività e le relative fasi da avviare in caso di Violazione del Dati Personali in conformità con quanto stabilito dagli Artt. 33 e 34 del Regolamento UE 2016/679 che stabiliscono i seguenti obblighi:

- Obbligo di notifica all'Autorità Garante "senza ingiustificato ritardo" e, ove possibile, entro 72 ore (art. 33 del Regolamento).
- 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 Regolamento).

5.1 Articolo 33 – Reg UE 2016/679 Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di **violazione dei dati personali**, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 (del Regolamento) 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 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, 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) comunicare 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) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere 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 all'autorità di controllo di verificare il rispetto del presente articolo.

5.2 Articolo 34 – Reg UE 2016/679 Comunicazione di una violazione dei dati personali all'interessato

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 di cui al paragrafo 1 del presente articolo 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 Regolamento), 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 di cui al paragrafo 1;

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, l'autorità di controllo 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 Gruppo di Risposta alle Violazioni ed elementi di valutazione

6.1 Gruppo di Risposta alle Violazioni

Il Gruppo di Risposta alle Violazioni è un soggetto multidisciplinare composto da professionalità che presentano conoscenze e competenze tali da assumere la responsabilità per valutare e per porre in essere le misure di contenimento delle conseguenze negative della violazione.

La composizione del Gruppo 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 Gruppo, da ulteriori referenti.

Gruppo di Risposta alle Violazioni		
Funzione	**Competenza**	**Partecipazione**
Data Protection Officer	Responsabile della Protezione dei Dati Personali	Componente di base
Direzione Generale	Apice della struttura organizzativa	Componente di base
UOSD Segreteria di Direzione	Utile per comunicazioni verso l'interno e verso l'esterno, sia per migliorare il coordinamento interno sia per un miglior interfacciamento verso i soggetti interessati e a conoscenza del quadro normativo nazionale ed europeo	Componente di base e Coordinatore gruppo
Resp. Transazione Digitale	Conoscenze tecnologiche, di informatica giuridica e manageriali, necessarie per il coordinamento nel percorso di semplificazione e crescita dell'ente. In fase di designazione la nomina	In base all'area organizzativa in cui si verifica l'evento
UOC Sistemi Informativi	Conoscenza dell'infrastruttura di rete, delle misure di sicurezza idonee adottate e delle infrastrutture tecnico-applicative impiegate per il trattamento dei dati	In base all'area organizzativa in cui si verifica l'evento
Direttore/Responsabile della struttura organizzativa in cui si è verificato l'evento	Possono fornire ulteriori informazioni e supporto per un efficace risposta all'incidente	In base all'area organizzativa in cui si verifica l'evento
UOC Patrimonio, Lavori e Manutenzioni (Ufficio Apparecchiature elettromedicali)	Conoscenza delle attrezzature Sanitarie di trattamento dati	Opzionale – Su richiesta

UOC Acquisizioni Beni e Servizi	Può fornire informazioni sui contratti/convenzioni qualora l'incidente riguardi un trattamento dati effettuato da un responsabile del trattamento	Opzionale – Su richiesta

Il soggetto che coordina il Gruppo di Risposta alle Violazioni sarà l' UOSD Segreteria di Direzione con il supporto del Responsabile della Protezione dei Dati (DPO)

Il Gruppo deve assicurare un'adeguata tempestività nella risposta alle violazioni, oltre a fornire le indicazioni necessarie per il contrasto degli effetti pregiudizievoli dell'evento.

Il Gruppo di Risposta alle Violazioni deve essere preparato alla risposta di presunti o accertate violazioni 24h/7g. A tal fine, è necessario avere a disposizione una lista dei numeri di contatto del Gruppo (si rinvia all'Allegato 4 "Gruppo di Risposta alle Violazioni").

6.1.1 Compiti del Gruppo

A valle della segnalazione della violazione, il Gruppo dovrà:

- Registrare l'incidente occorso nell'apposito registro su file o software appositamente predisposti
- Effettuare una valutazione dei rischi per i diritti degli interessati e dell'impatto sugli stessi
- Implementare tutte le misure di mitigazione possibili per alleviare nell'immediato ogni effetto negativo sugli interessati conseguente alla violazione
- 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 nel registro
- Implementare tutte le misure di mitigazione possibili per evitare che simili incidenti accadano nuovamente

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) Tipologia violazione: la tipologia di violazione si configura come parametro per la valutazione del rischio. (es. la violazione dei dati sanitari di tutti i pazienti è più grave della perdita dei dati sanitari di un paziente);
b) Natura, numero e grado di sensibilità dei dati personali violati;
c) Facilità di associazione dei dati violati all'interessato: facilità di associazione dei dati violati ad una determinata persona fisica;

d) Gravità delle conseguenze per gli interessati: valutazione relativa al rischio che i dati personali violati rappresentino un rischio immediato per gli interessati, tale da porre in essere frodi o sostituzioni di persona;
e) Numero di interessati esposti al rischio;
f) Caratteristiche del titolare del trattamento

In particolare per Tipologie di Violazioni si intende:

- Violazione sulla Riservatezza (cd. *Confidentiality Breach*) accesso accidentale o illecito ai dati personali o divulgazione degli stessi;
- Violazione sulla Disponibilità (cd *Availability Breach*) perdita o distruzione accidentale o illecita del dato personale;
- Violazione sull'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 le attività 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):
  - Analisi preliminare delle segnalazioni
  - Risk assessment, individuazione misure e contenimento della violazione
- 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 per canali interni ed esterni; è previsto un indirizzo di posta elettronica al quale poter comunicare la sospetta violazione: protezionedati@aslteramo.it (è un alias che può inoltrare a più indirizzi)

1) Canali interni

Le segnalazioni di eventi anomali possono provenire internamente da:

Personale dell'organizzazione: le violazioni di dati personali comunicate alla Direzione, sono istruite dall'ufficio per la protezione dei dati personali, con la supervisione della UOSD Segreteria di Direzione o di un

referente in materia privacy e con il supporto del Responsabile della Protezione dei Dati (DPO), con l'affiancamento del Direttore dell'UOC Sistemi Informativi o suo delegato, in caso di violazione di dati informatici. 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 Soggetto Autorizzato al Trattamento dei Dati di II livello si accorga di una concreta, potenziale o sospetta violazione dei dati personali, deve immediatamente informare il proprio responsabile/dirigente, Soggetto Autorizzato al Trattamento di I livello, della possibile violazione. Quest'ultimo, previo contatto telefonico, dovrà informare la UOSD Segreteria di Direzione, l'UOC Sistemi Informativi mediante la compilazione dell'Allegato 1 – Modulo di documentazione interna della Violazione da inviare tramite e-mail agli indirizzi presenti nella tabella di cui all'Allegato 4, senza ingiustificato, di ogni violazione della sicurezza che comporti 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.

UOC Sistemi Informativi mediante opportuni strumenti di monitoraggio di eventi di natura Software e ICT: le violazioni di dati possono emergere dal monitoraggio 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 dall'UOC Sistemi Informativi 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 della UOC Sistemi Informativi, la UOSD Segreteria di Direzione ed il Responsabile Protezione Dati (DPO) mediante la compilazione dell'Allegato 1 – Modulo di documentazione interna della Violazione da inviare tramite e-mail agli indirizzi presenti nella tabella di cui sopra.

2) Canali esterni

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

Segnalazione dall'interessato: l'interessato dal trattamento 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 all'organizzazione per la verifica di eventuali violazioni secondo quanto disposto dall'informativa ex art. 13 e quanto indicato sul sito.

Segnalazione dal Responsabile del Trattamento: il Responsabile del Trattamento, in caso si accorga di una concreta, potenziale o sospetta violazione dei dati personali, deve immediatamente informare il proprio referente presso la ASL della possibile violazione mediante la compilazione dell'Allegato 1 – Modulo di documentazione interna della Violazione da inviare tramite e-mail agli indirizzi presenti nella tabella di cui sopra.

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, individuazione misure e contenimento della violazione
3) Eventuale Notifica all'Autorità Garante
4) Eventuale comunicazione agli interessati

7.2.1 Analisi preliminare delle segnalazioni

La struttura incaricata della valutazione delle segnalazioni di Violazioni di Dati Personali è il cosiddetto Gruppo di Risposta alle Violazioni di cui al punto 6.1 che effettuerà una analisi preliminare sulle informazioni relative alla presunta violazione, raccolte attraverso l'apposito modulo (Allegato 1), avendo in tal modo un quadro strutturato sull'anomalia segnalata.
A seguito della ricezione della segnalazione, compilata tramite l'Allegato 1, il Titolare del trattamento, per il tramite della UOSD Segreteria di Direzione con il supporto del Responsabile della Protezione dei Dati (DPO), effettua la registrazione e l'identificazione univoca della segnalazione, quindi, assieme alla UOSD Segreteria di Direzione e alla UOC Sistemi Informativi, in caso di violazione di dati informatici, effettuerà una valutazione preliminare riguardante la possibile violazione occorsa, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di Violazione e se sia necessaria un'indagine più approfondita dell'accaduto avviando la fase di risk assessment (par. 7.2.2).
Nel caso in cui l'evento venga accertato come "falso positivo", la procedura di verifica viene chiusa e l'evento viene classificato all'interno del registro delle Violazioni (Allegato 2 – Fac simile di Registro Segnalazioni per le Violazioni) nell'apposita sezione relativa agli eventi falsi positivi.
Nel caso in cui la violazione venga accertata, il Gruppo procede al recupero di quante più informazioni possibili relative alla violazione per la gestione dell'evento ed informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
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;
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 (ICT), il Responsabile dell'UOC Sistemi Informativi inoltrerà la segnalazione al Responsabile Protezione Dati e

all'Amministratore di Sistema di competenza per effettuare una istruttoria e le valutazioni in merito all'accaduto.
Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nell'Allegato 1, 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.

7.2.1.1 Azioni di Contenimento

Alcune *best practices* da attuare come primo approccio alle violazioni sono quelle elencate di seguito. Nel caso di eventi che coinvolgano sistemi ICT, tali *best practices* non sono esaustive dell'attività da mettere in pratica ma costituiscono un buon punto di partenza:

1. Contenere i dispositivi compromessi mettendoli offline
2. Censire le macchine che sono state violate
3. Individuare quali vulnerabilità siano state sfruttate per violare i dispositivi ed eventualmente gli apparati di rete
4. Raccogliere evidenze per il Garante in modo tale da dimostrare quali misure siano state impiegate e quali azioni siano state attuate durante l'evento
5. Ripristinare i sistemi e le reti
6. Integrare le informazioni raccolte per individuare nuove misure al fine di stabilire un nuovo piano per far sì che l'incidente non avvenga in futuro

Nel caso di violazioni di dati cartacei, le *best practices* sono senz'altro da individuarsi nella corretta applicazione dei regolamenti interni e/o le disposizioni della direzione e nella continua formazione del personale.

7.2.2 Risk assessment e individuazione delle misure

Al termine della fase di valutazione preliminare, nel caso si stabilisca che una possibile violazione è effettivamente avvenuta, il Gruppo di risposta alle Violazioni stabilisce:

- le opportune misure correttive e di protezione che possano limitare i danni che la violazione potrebbe causare;
- 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 l'accadimento agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Gruppo di lavoro alle Violazioni valuterà la gravità della violazione utilizzando un modello standardizzato,

come da Modulo di valutazione del Rischio connesso alla Violazione (Allegato 3), secondo le indicazioni di cui all'art. 33 GDPR. Si precisa che gli obblighi di notifica all'Autorità di Controllo scaturiscono soltanto quando il Titolare del trattamento ritenga probabile che dalla violazione derivino rischi per i diritti e le libertà degli interessati.

L'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio elevato, con l'eccezione di alcune ipotesi. Non è richiesta la comunicazione all'interessato quando è presente una delle seguenti condizioni: 1) 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; 2) 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; 3) la 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.

7.2.3 Eventuale 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, il Titolare del trattamento della ASL Teramo per il tramite della UOSD Segreteria di Direzione con il supporto del Responsabile della Protezione dei Dati (DPO), provvederanno alla notifica all'Autorità Garante senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.

La notifica al Garante (come di seguito strutturata), da secondo la procedura al momento messa a disposizione dagli organi competenti, dovrà contenere, a titolo esemplificativo e non esaustivo:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, 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) comunicare 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) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere 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.

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

7.2.4 Eventuale Comunicazione agli interessati

Se a seguito delle valutazioni preliminari e del risk assessment effettuato nel rispetto della presente procedura, è stata valutata la necessità di effettuare la comunicazione della violazione dei dati agli interessati, in quanto è stato riscontrato un rischio elevato per i diritti e le libertà delle persone fisiche, secondo quanto

prescritto dal Regolamento (UE) 2016/679, il Titolare del trattamento per il tramite della UOSD Segreteria di Direzione con il supporto del Responsabile della Protezione dei Dati (DPO), procede alla comunicazione all'Interessato senza ingiustificato ritardo.

Il contenuto della comunicazione prevede:

- Una descrizione chiara e facile da comprendere dell'accaduto;
- Una descrizione delle probabili conseguenze della violazione dei dati personali;
- Una descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento dovrà sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali mail o comunicazioni dirette).

Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, si potrà utilizzare una comunicazione pubblica, 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 GDPR dovrà descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e conterrà almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del Regolamento UE 2016/679.

Secondo quanto previsto dall'art. 34.3 del Regolamento UE 2016/679, nei seguenti casi non è richiesta la comunicazione all'interessato:

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 di cui al paragrafo 1;*
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.*

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo 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 all'art. 34.3 sia soddisfatta.

7.3 Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere alla notificazione e/o comunicazione della violazione di dati personali, ogni qualvolta si verifichi un incidente comunicato dagli attori che partecipano al trattamento attraverso l'Allegato 1, la ASL sarà tenuta a documentarlo.

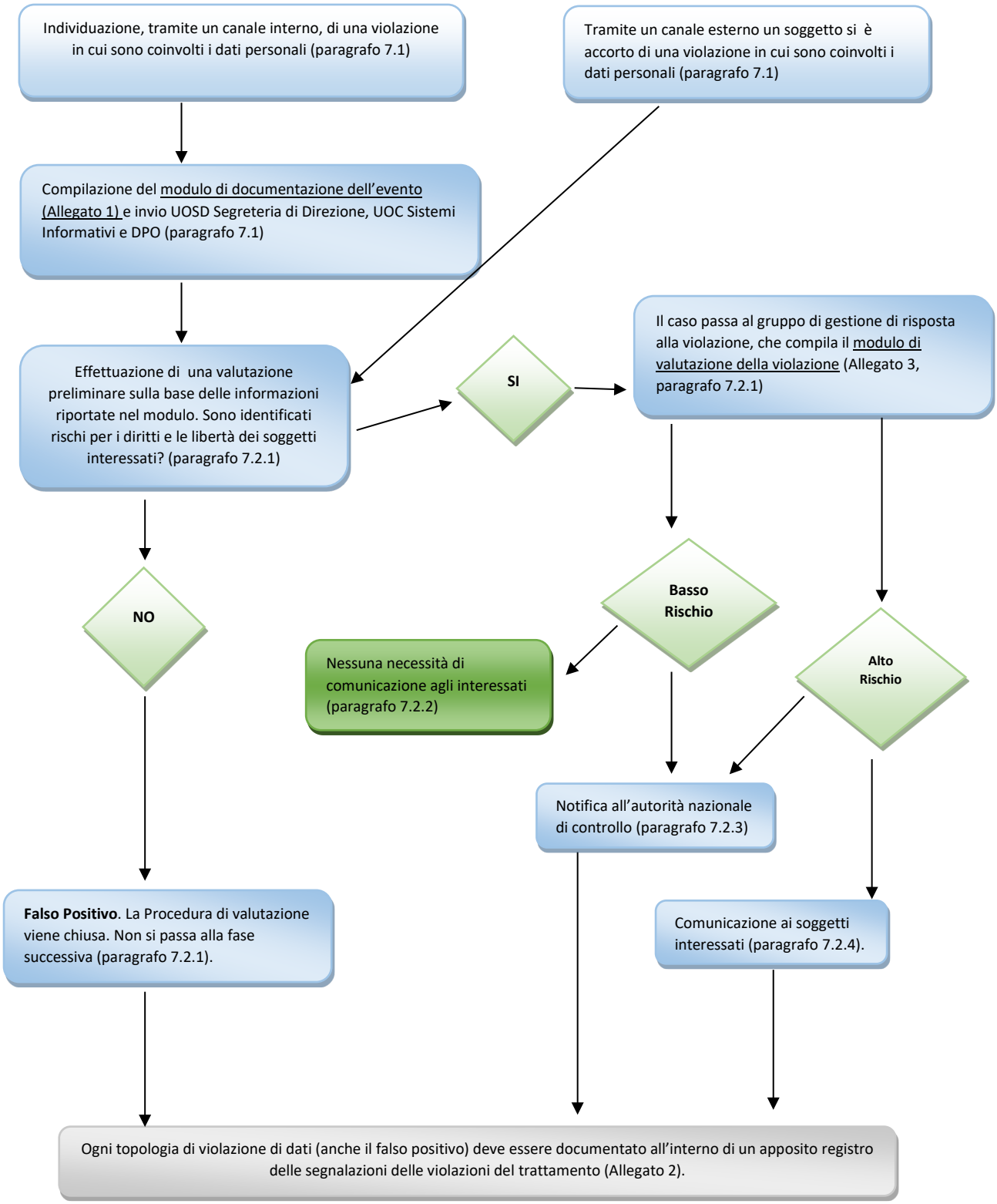
A tal fine il Titolare provvede per il tramite della UOSD Segreteria Di Direzione o di altro ufficio del gruppo di risposta, con il supporto del Responsabile della Protezione dei Dati a compilare il Registro delle Violazioni (Allegato 2 – Fac simile di Registro Segnalazioni per le Violazioni), in cui saranno riportate le seguenti informazioni:

- n. segnalazione;
- data segnalazione;
- segnalatore;
- valutazione;
- notifica all'Autorità Garante Privacy;
- comunicazione agli interessati.

Il Registro delle Violazioni (Allegato 2 – Fac simile di Registro Segnalazioni per le Violazioni) potrà essere tenuto anche in formato elettronico con il supporto di applicativi software, sarà continuamente aggiornato e messo a disposizione del Garante qualora richieda di accedervi.

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.


Individuazione, tramite un canale interno, di una violazione in cui sono coinvolti i dati personali (paragrafo 7.1)
Tramite un canale esterno un soggetto si è accorto di una violazione in cui sono coinvolti i dati personali (paragrafo 7.1)
Compilazione del modulo di documentazione dell'evento (Allegato 1) e invio UOSD Segreteria di Direzione, UOC Sistemi Informativi e DPO (paragrafo 7.1)
Effettuazione di una valutazione preliminare sulla base delle informazioni riportate nel modulo. Sono identificati rischi per i diritti e le libertà dei soggetti interessati? (paragrafo 7.2.1)
SI
Il caso passa al gruppo di gestione di risposta alla violazione, che compila il modulo di valutazione della violazione (Allegato 3, paragrafo 7.2.1)
NO
Basso Rischio
Alto Rischio
Nessuna necessità di comunicazione agli interessati (paragrafo 7.2.2)
Notifica all'autorità nazionale di controllo (paragrafo 7.2.3)
Falso Positivo. La Procedura di valutazione viene chiusa. Non si passa alla fase successiva (paragrafo 7.2.1).
Comunicazione ai soggetti interessati (paragrafo 7.2.4).
Ogni topologia di violazione di dati (anche il falso positivo) deve essere documentato all'interno di un apposito registro delle segnalazioni delle violazioni del trattamento (Allegato 2).

8 Violazione dei dati presso l'Azienda quando opera in qualità di Responsabile del Trattamento

8.1 Obblighi di comunicazione dell'Azienda quando opera in qualità di responsabile

Qualora l'Azienda agisca in qualità Responsabile del Trattamento, in caso di Violazione dei Dati Personali, sarà tenuta ad informare il Titolare del trattamento senza ingiustificato ritardo secondo i tempi e i modi concordati nel contratto per il trattamento dei dati personali trasmesso da quest'ultimo.

9 Allegati

9.1 Allegato 1 - Modulo di documentazione interna della Violazione

Modulo di documentazione interna della Violazione di Dati Personali	
Nome soggetto che riporta l'incidente	
Unità Operativa di appartenenza	
Numero di contatto del soggetto che riporta l'incidente ed indirizzo di posta elettronica	
Data dell'evento ed orario (anche approssimativo)	
Data e ora in cui si è venuti a conoscenza della violazione	
Fonte della segnalazione	
Tipologia di anomalia riscontrata	
Descrizione dell'anomalia	
Numero di soggetti coinvolti	

Numero dei dati personali di cui si presume il coinvolgimento	
Tipologia di dati personali che si ritiene essere stati coinvolti	**Basso Rischio**:
	Alto Rischio: i dati identificano *(barrare con X)* • razza o origine etnica • opinioni politiche, religiose o filosofiche • appartenenza a sindacati • dati genetici • dati biometrici • dati che identificano orientamento sessuale • dati che riguardano la salute
Modalità in cui è avvenuta la violazione (es. avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)	
Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	
Azioni poste in essere (Contenimento)	

9.2 Allegato 2 – Fac simile di Registro Segnalazioni per le Violazioni

ESTREMI SEGNALAZIONE			ESITO		NOTIFICA GARANTE		COMUNICAZIONE AGLI INTERESSATI	
Num.	**Data**	**Unità Operativa**	**Valutazione**	**Falso positivo**	**Effettuata**	**Data Notifica**	**Effettuata**	**Data Comunicazione**

9.3 Allegato 3 – Modello di valutazione della segnalazione

	Tipologia di violazione		Rischio			
Tip. Operaz.	**Accidentale**	**Illecito**	**Basso**	**Medio**	**Alto**	**Critico**
Accesso						
Modifica						
Perdita						
Distruzione						
Divulgazione						

Nel modello sopra indicato, è necessario indicare con una "X" la tipologia di operazione eseguita in relazione alla tipologia di violazione; successivamente deve essere indicato, in maniera corrispondente il livello di rischio dell'evento verificatosi considerando i seguenti criteri di valutazione/gravità:

- **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 8 ore e non oltre le 24 ore);
- **4 – Rischio Critico**: gli interessati coinvolti dal trattamento possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (es.: Interruzione del servizio oltre le 24 ore, impossibilità o perdita della possibilità di accesso ai servizi, mancato rispetto dei diritti dell'interessato – es.: diritto alla salute)

Una volta individuato il livello di rischio dell'evento verificatosi, dovranno essere attuate le seguenti istruzioni:

- 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 critico**, la violazione deve essere comunicata sia al Garante Privacy che all'interessato.

9.4 Allegato 4 – Gruppo di Risposta

Indirizzo per la segnalazione di violazione di dati:

protezionedati@aslteramo.it

Funzione	Contatto mail ordinaria	Telefono
Uosd Segreteria di Direzione	uosdsegreteria@aslteramo.it	0861 – 420223
Dpo	dpo@aslteramo.it	3482248440
UOC Sistemi Informativi	sistemi.informativi@aslteramo.it	0861 420371,382
Direzione Generale	Direzione.generale@aslteramo.it	0861 420 203,204