AZIENDA SANITARIA LOCALE AVELLINO

ORIGINALE ☐

COPIA ☐

IL DIRETTORE GENERALE

Deliberazione n. 349 **del** 25-03-2019

PUBBLICAZIONE

Dichiarazione di conformità del trattamento dei dati ex D.Lgs. n. 196/2003 e ss.mm.ii.

Premesso che il D.l.vo196/2003 e ss.mm.ii. contiene principi e prescrizioni per il trattamento dei dati personali, anche con riferimento alla loro "diffusione", il Proponente la presente deliberazione dichiara di aver valutato la rispondenza del testo, compreso degli eventuali allegati, destinato alla diffusione per il mezzo dell'Albo Pretorio alle suddette prescrizioni e ne dispone la pubblicazione nei modi di legge.

(firma del proponente)

OGGETTO: Regolamento UE 2016/679 artt. 33 e 34 - Approvazione procedura per la gestione degli incidenti di sicurezza con o senza violazione dei dati personali (data breach – near miss)

ATTESTATO PUBBLICAZIONE

Si attesta che la presente deliberazione è stata affissa all'Albo Pretorio il giorno: 26 MAR. 2019

ai sensi dell'art.124 c.1 D.L.vo 267/2000, per giorni 15

Il Responsabile Ufficio Delibere e Determine

DICHIARAZIONE DI REGOLARITÀ CONTABILE:

il presente atto trova capienza di spesa all'autorizzazione :
n. del
n. del
n. del

In presenza di fattura di importo superiore a € 5.000,00, prima dell'emissione del relativo mandato di pagamento l'UOC Contabilità Generale effettuerà il controllo tramite l'Agenzia delle Entrate.

Il Direttore U.O.C Contabilità Generale

☒ Il presente provvedimento è reso immediatamente esecutivo.

IL DIRETTORE GENERALE

Dr.ssa Maria Morgante

PROPOSTA DI DELIBERA

Oggetto: Regolamento UE 2016/679 artt. 33 e 34 - Approvazione procedura per la gestione degli incidenti di sicurezza con o senza violazione dei dati personali (data breach – near miss)

La Dott.ssa Alessandra Antocicco, in qualità di Responsabile dell'U.O.S.D. Rapporti con Organi e Organismi aziendali

VISTI

- il D. Lgs. 196/2003 e s.m. i;
- il Regolamento UE 2016/679 (GDPR) ed in particolare gli artt. 33 e 34 che disciplinano la fattispecie di violazione dei dati personali e gli eventuali successivi adempimenti di notifica all'autorità di controllo e di comunicazione agli interessati;

RITENUTO, a tal fine, opportuno approntare una procedura aziendale che, al verificarsi di un incidente di sicurezza, disciplini tutte le azioni e i relativi soggetti responsabili, al fine di:

- valutare se l'incidente sia un'effettiva violazione dei dati personali (data breach) o una quasi violazione (near miss) stabilendo per le due diverse ipotesi tutte le azioni necessarie;
- approntare dei format, da utilizzare nelle strutture aziendali, nelle varie fasi sopra delineate;
- istituire il Registro degli incidenti di sicurezza, contenente al suo interno, le violazioni dei dati personali di cui agli artt. 33 e 34 del GDPR;

VISTA la procedura a tal fine predisposta, allegata al presente atto a costituirne parte integrante e sostanziale

PRECISATO che detta procedura sarà suscettibile di aggiornamento a seguito di emanazione di appositi provvedimenti in materia;

DATO ATTO CHE tutta la documentazione originale a supporto del presente atto è depositata e custodita presso l'U.O.S.D. proponente;

DICHIARATA la regolarità giuridico amministrativa della presente proposta di provvedimento, a seguito dell'istruttoria effettuata, nel rispetto delle proprie competenze, funzioni e responsabilità;

DICHIARATO che il presente provvedimento non comporta alcun impegno di spesa e che non sussistono motivi ostativi a procedere, attesa la piena conformità alle disposizioni di legge e ai regolamenti aziendali;

Tutto ciò premesso, argomentato ed attestato, il sottoscritto Direttore

PROPONE AL DIRETTORE GENERALE

l'adozione del presente provvedimento e, nello specifico, per i motivi espressi in narrativa e che qui si intendono per trascritti e confermati :

di approvare la procedura aziendale che, al verificarsi di un incidente di sicurezza, disciplini tutte le azioni e i relativi soggetti responsabili, al fine di valutare se l'incidente sia un'effettiva violazione dei dati personali (data breach) o una quasi violazione (near miss) stabilendo per le due diverse ipotesi tutte le azioni necessarie;

di approvare i format, allegati alla procedura di cui al precedente punto, da utilizzare nelle strutture aziendali, nelle varie fasi come delineate nella stessa;

di istituire il Registro degli incidenti di sicurezza, contenente al suo interno, le violazioni dei dati personali di cui al punto 9 della procedura in oggetto;

- **di precisare** che detti documenti saranno suscettibili di aggiornamento a seguito di emanazione di appositi provvedimenti in materia;
- **di pubblicare** il presente atto sul sito web aziendale nell'apposita sezione PRIVACY;

Estensore
Alessandra Antocicco

Responsabile U.O.S.D. Raporti con Organi e Organismi aziendali
Dr.ssa Alessandra Antocicco

IL DIRETTORE GENERALE

dell'Azienda Sanitaria Locale Avellino, Dott.ssa Maria Morgante, nominato con D.G.R.C. n. 427 del 27/07/2016 e immesso nelle funzioni con D.P.G.R.C. n.179 del 01/08/2016, coadiuvato dal Direttore Sanitario Dr.ssa Emilia Anna Vozzella ha adottato la seguente delibera:

Vista
la suesposta proposta del Responsabile dell'U.O.S.D. Rapporti con Organi e Organismi aziendali avente ad oggetto: Regolamento UE 2016/679 artt. 33 e 34 - Approvazione procedura per la gestione degli incidenti di sicurezza con o senza violazione dei dati personali (data breach – near miss)

Preso atto
- dell'espressa dichiarazione di regolarità giuridico amministrativa resa dal Responsabile dell'U.O.S.D. Rapporti con Organi e Organismi aziendali, a seguito della istruttoria dallo stesso effettuata e come dallo stesso attestato ed articolato;
- di tutto quanto riportato nella proposta di delibera ;

Ritenuto
Di prendere atto, quale parte integrante e sostanziale del presente provvedimento, della suesposta proposta resa dal Responsabile dell'U.O.S.D. Rapporti con Organi e Organismi aziendali sulla scorta ed in conformità della stessa ;

Con il parere favorevole reso, alla luce di tutto quanto sopra riportato ed attestato, dal Direttore Sanitario con la sottoscrizione della presente proposta di provvedimento;

Il Direttore Sanitario
Dr.ssa Emilia Anna Vozzella

DELIBERA

di prendere atto, quale parte integrante e sostanziale del presente provvedimento, della suesposta proposta resa dal Responsabile dell'U.O.S.D. Rapporti con Organi e Organismi aziendali e sulla scorta ed in conformità della stessa:

- **di approvare** la procedura aziendale che, al verificarsi di un incidente di sicurezza, disciplini tutte le azioni e i relativi soggetti responsabili, al fine di valutare se l'incidente sia un'effettiva violazione dei dati personali (data breach) o una quasi violazione (near miss) stabilendo per le due diverse ipotesi tutte le azioni necessarie;
- **di approvare** i format, allegati alla procedura di cui al precedente punto, da utilizzare nelle strutture aziendali, nelle varie fasi come delineate nella stessa;
- **di istituire** il Registro degli incidenti di sicurezza, contenente al suo interno, le violazioni dei dati personali di cui al punto 9 della procedura in oggetto;
- **di precisare** che detti documenti saranno suscettibili di aggiornamento a seguito di

emanazione di appositi provvedimenti in materia;

- **di pubblicare** il presente atto sul sito web aziendale nell'apposita sezione PRIVACY;
- **di trasmettere** il presente atto al Collegio Sindacale, e a tutte le strutture aziendali

Il Direttore Generale
Dr.ssa Maria Morgante

PROCEDURA PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA CON O SENZA VIOLAZIONE DEI DATI PERSONALI

(DATA BREACH - NEAR MISS)

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

Sommario

1. INTRODUZIONE

Il Regolamento UE 2016/679 (GDPR) prevede, in capo al Titolare delle attività di trattamento, l'obbligo di tutelare la riservatezza dei dati personali al fine di evitare che un loro uso non corretto o una violazione degli stessi possa ledere i diritti e le libertà fondamentali degli interessati, nonché la loro dignità.

La Azienda Sanitaria Locale (ASL), per definizione, tratta dati ad alto rischio potenziale per la sicurezza, atteso che la quasi totalità delle attività di trattamento comporta la necessità di trattare dati comuni e particolari (in special modo quelli idonei a rivelare lo stato di salute) e, a volte, quelli giudiziari o di altra natura, quali quelli di disagio sociale, indispensabili per assicurare l'erogazione e la gestione delle prestazioni richieste.

A tal proposito la letteratura in materia di rischi e misure di sicurezza in tema di trattamento dei dati ha evidenziato che in sanità, per la tipologia dei dati trattati e la complessità dei processi organizzativi supportati da Information Communications Technology (ICT), è altamente probabile che la maggior parte dei trattamenti siano a "rischio elevato".

Al fine di garantire un buon livello di sicurezza, oltre che per rispondere ad un preciso obbligo previsto dal legislatore, la ASL ha elaborato il presente documento, finalizzato a disciplinare la procedura aziendale da porre in essere nell'eventualità in cui si verifichi un incidente di sicurezza sul trattamento dei dati, sia in caso di violazioni concrete (data breach) sia nel caso di quasi violazioni di dati personali (near miss). La presente procedura tiene conto delle tempistiche previste dalla normativa per le comunicazioni all'Autorità Garante e/o agli interessati al fine di assicurarne il rispetto.

2. NORMATIVA DI RIFERIMENTO

- **Regolamento UE 2016/679 del 27.04.2016** 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;
- **Decreto Legislativo 30.06.2003 n. 196** "Codice in materia di protezione dei dati personali"
- **Decreto Legislativo 10.08.2018 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";
- **Scheda informativa del Garante** per la protezione dei dati personali del **14 dicembre 2018** "Violazioni di dati personali (data breach), in base alle previsioni del Regolamento (UE) 2016/679";
- **Linee Guida del Gruppo di Lavoro Articolo 29** per la protezione dei dati sulla notifica delle violazioni dei dati personali, ai sensi del regolamento UE 2016/679, adottate il 3.10.2017 nella versione emendata e adottata in data **6.2.2018**;
- **Provvedimento Garante** per la protezione dei dati personali in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) - 4 aprile 2013;
- **Provvedimento generale Garante** per la protezione dei dati personali prescrittivo in tema di biometria - 12 novembre 2014;
- **Linee guida Garante** per la protezione dei dati personali in materia di Dossier sanitario - 4 giugno 2015;
- **Provvedimento Garante** per la protezione dei dati personali Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015.

3. SCOPO E AMBITO DI APPLICAZIONE

La presente procedura operativa della ASL Avellino per la gestione degli incidenti di sicurezza, con o senza violazione dei dati personali, garantisce il rispetto degli artt. 33 e 34 del Regolamento UE.
La procedura si applica a tutte le strutture aziendali che trattano, a qualsiasi titolo ed in qualsiasi modalità, dati personali riconducibili alle attività aziendali.

Ai sensi dell'art. 4 punto 12 del Regolamento si definisce **"violazione di dati" o "data breach"** "*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*".
Si definisce **"near miss" o "quasi violazione"** qualsiasi evento, correlato al trattamento dei dati, che avrebbe potuto causare una violazione degli stessi ma, solo per puro caso, non l'ha prodotta: un evento, quindi, che ha in sé la potenzialità di produrre una violazione.

Le "quasi violazioni", proporzionalmente molto più numerose delle violazioni, vanno considerate, al pari delle violazioni vere e proprie, indicatori di rischio.
Tale procedura si applica, pertanto, a tutte le operazioni di trattamento, a tutti gli archivi, a tutti i documenti e a tutti i sistemi, cartacei e/o informatici, su cui sono presenti dati personali degli interessati che l'Azienda tratta direttamente o con il supporto di Responsabili ex art. 28 del Regolamento e/o ex art.2-quaterdecies del D.Lvo 196/2003 e ss.mm.ii..
Ogniqualvolta, infatti, l'Azienda/Titolare del trattamento si trovi ad affidare un'attività che comporta anche il trattamento di dati personali ad un soggetto terzo o responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico accordo che lo vincoli al rispetto delle istruzioni impartitegli dal titolare in materia di protezione dei dati, compresa la presente procedura di segnalazione di *data breach*. Ciò al fine di obbligare il responsabile ad informare il Titolare del trattamento, senza ingiustificato ritardo, di ogni incidente di sicurezza, concreto o potenziale evento di *data breach*.

4. RUOLI E RESPONSABILITA'

Nella seguente tabella si riepilogano ruoli e responsabilità dei vari attori coinvolti nella presente procedura:

SOGGETTI	RUOLO PREVISTO PER NORMATIVA	RESPONSABILITA' PER PROCEDURA
TITOLARE	ruolo istituzionale: titolare degli adempimenti previsti per legge	supervisione delle attività, approvazione dei documenti prodotti, decisioni di competenza nel corso della procedura. Se necessario, notifica dell'incidente all'Autorità Garante e agli interessati
RESPONSABILE PROTEZIONE DATI (RPD)	ruolo istituzionale: supporto tecnico al titolare del trattamento per il corretto indirizzamento delle decisioni nell'ambito della procedura di gestione della violazione	supporto giuridico alle decisioni del titolare e a tutti gli altri soggetti nell'attuazione delle operazioni di valutazione
RESPONSABILE UOSD ROOA (Rapporto con organi e organismi aziendali)	ruolo aziendale: trattamento all'interno della Azienda della materia privacy e, quindi, anche della violazione della sicurezza	coordinamento del processo di gestione delle violazioni della sicurezza dei dati
DIRETTORE UOC SIA	ruolo aziendale: responsabile all'interno della Azienda della gestione software e ICT in particolare dello svolgimento delle attività di monitoraggio, rilevamento degli eventi che rappresentano violazione della privacy o che costituiscono un allarme di presunta violazione privacy	monitoraggio, analisi, classificazione e gestione degli eventi che possano generare allarme di sicurezza ICT o che costituiscano violazione con impatto sulla privacy; inoltro tempestivo al Titolare delle segnalazioni di potenziale violazione dei dati e collaborazione nelle attività di valutazione preliminare
AMMINISTRATORE DI SISTEMA (anche se esterno)	ruolo aziendale: responsabile della gestione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise Resource Planning), delle reti locali e degli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali	responsabile dell'inoltro tempestivo al Titolare delle segnalazioni di potenziale violazione dei dati e collaborazione nelle attività di valutazione preliminare
Direttori, Responsabili strutture aziendali	ruolo aziendale: responsabili delle attività afferenti alla propria struttura e quindi anche della corretta gestione privacy dei dati	responsabili dell'inoltro tempestivo delle segnalazioni di potenziale violazione e collaborazione nelle attività di valutazione preliminare.
Tutti i dipendenti aziendali di ruolo non apicale	ruolo aziendale: "autorizzati" al trattamento dei dati relativamente alle attività da loro effettuate e con i profili loro attribuiti dal Direttore/Responsabile secondo una corretta gestione privacy dei dati	responsabili della segnalazione immediata al proprio dirigente responsabile dell'evento, ai fini del successivo inoltro al titolare nel rispetto della presente procedura
RESPONSABILI ESTERNI	ruolo istituzionale: espletamento attività per conto del Titolare che comportano il trattamento dei dati personali	responsabili dell'inoltro tempestivo delle segnalazioni di potenziale violazione al Titolare e collaborazione nelle attività di valutazione preliminare.
TERZO ex art. 2-quaterdecies del D.Lvo 196/2003	ruolo istituzionale: espletamento attività per conto del Titolare che comportano il trattamento dei dati personali	responsabili dell'inoltro tempestivo al Titolare delle segnalazioni di potenziale violazione e collaborazione nelle attività di valutazione preliminare.

5. TIPOLOGIE DI VIOLAZIONI DEI DATI

Per l'individuazione dell'effettiva violazione dei dati personali è necessario procedere ad una classificazione del Rischio e della tipologia di Eventi.

5.1 CLASSIFICAZIONE RISCHIO

Le violazioni dei dati personali si considerano tali se hanno un reale impatto sulla ***riservatezza, integrità o disponibilità*** dei dati personali degli interessati (cittadini, dipendenti, soggetti terzi ecc.).
Di seguito una breve descrizione delle varie tipologie di rischio di violazione dei dati personali:

5.1.1 Rischio di indisponibilità dei dati

a) **Distruzione:** Indisponibilità definitiva di dati personali degli interessati con impossibilità di ripristino degli stessi entro sette giorni. La violazione può essere determinata da una eliminazione logica (es. cancellazione dei dati) oppure fisica (es. rottura dei supporti di memorizzazione) non autorizzata e relativa impossibilità di ripristinare i dati entro i sette giorni.

b) **Perdita:** Perdita del supporto fisico di memorizzazione dei dati (dischi esterni, pendrive ecc.) in termini di privazione, smarrimento dei dispositivi contenenti i dati degli interessati oppure dei documenti cartacei. La perdita può essere anche temporanea ma superiore a sette giorni. Può riguardare le copie o gli originali dei supporti contenenti i dati personali dei soggetti interessati.

c) **Furto:** sottrazione fraudolenta di dati personali contenuti nel supporto fisico di memorizzazione dei dati oppure dei documenti cartacei. Può riguardare le copie o gli originali dei documenti cartacei o dei supporti contenenti i dati personali dei soggetti interessati .

5.1.2 Rischio di integrità dei dati

d) **Alterazione/Modifica:** Modifiche improprie dei dati degli interessati non autorizzate, effettuate al di fuori dei processi operativi di trattamento dei dati svolti dagli incaricati autorizzati, oppure modifiche con finalità fraudolente eseguite dagli autorizzati all'accesso.

5.1.3 Rischio di riservatezza dei dati

e) **Rivelazione:** Distribuzione non autorizzata o impropria dei dati personali degli interessati verso terze parti (persone fisiche, persone giuridiche, gruppi di soggetti, pubblico) anche non precisamente identificabili.

f) **Accesso abusivo:** Accesso non autorizzato o improprio ai dati degli interessati. Accessi ai dati (anche in sola visualizzazione, sia in caso di accessi logici ai sistemi informatici sia agli archivi cartacei) effettivamente avvenuti al di fuori dei processi operativi di trattamento dei dati previsti e autorizzati.

g) **Trattamento non conforme:** utilizzo dei dati al di fuori dei processi operativi e finalità autorizzate.

5.2 CLASSIFICAZIONE EVENTI

La ASL ha individuato, in maniera esemplificativa e non esaustiva, una classificazione dei possibili eventi causa delle violazioni dei dati personali sopra specificate. Il verificarsi di uno degli eventi di seguito descritti non costituisce tuttavia condizione sufficiente per stabilire, in automatico, l'effettiva violazione (Data Breach).

5.2.1 Eventi Accidentali da trattamenti elettronici

Eventi anomali determinati da fatti fortuiti che causano la perdita delle caratteristiche di sicurezza dei dati personali degli interessati (confidenzialità, integrità o disponibilità) in caso di trattamenti informatizzati.
Rientrano in tali casistiche eventi generati nella gestione dei sistemi ICT (gestiti internamente oppure in outsourcing) quali:

- **Esecuzione erronea di comandi e/o procedure per distrazione,** ad esempio:
  - pubblicazione erronea delle informazioni personali (non di dominio pubblico) su portali web pubblici;

- erroneo invio di informazioni a enti esterni alla ASL;
- formattazione di dispositivi di memorizzazione;
- errori nell'implementazione di una policy di controllo e verifica periodica delle abilitazioni degli accessi;
- divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato.

- **Rottura delle componenti HW,** a titolo di esempio:
  - distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura e/o di elettricità, di umidità, di corto circuito,
  - caduta accidentale,
  - eventi catastrofici/incendi, ecc.

- **Malfunzionamenti Software,** ad esempio:
  - esecuzione di uno script automatico non autorizzato;
  - errori di programmazione che causano output errati.

- **Visibilità errata di dati sul sito web dell' ASL,** ad esempio:
  - visibilità da parte di utenti di dati di altri interessati anche per casi di omonimia.

- **Fornitura dati a persona diversa dall'interessato,** a titolo di esempio:
  - comunicazioni di dati di interessati a destinatari errati;
  - gestione di informazioni avanzate da persone diverse dal Titolare o suo delegato;

- **Guasti alla rete aziendale,** a titolo di esempio:
  - caduta delle comunicazioni durante il trasferimento di dati e conseguente perdita di dati durante la trasmissione, ecc.

5.2.2 Eventi Dolosi da trattamenti elettronici

Eventi dolosi causati da personale interno o soggetti esterni realizzati tramite:

- **accesso non autorizzato** ai dati con lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione ad esempio:
  - furto di supporti di memorizzazione e/o elaborazione contenenti dati personali degli interessati (es: furto laptop, hard disk, chiavette USB, smartphone, tablet ecc)

- **compromissione o rivelazione abusiva** di credenziali di autenticazione;

- **utilizzo di software malevolo**. In tale casistica rientrano gli incidenti di sicurezza ICT che comportano la violazione dei dati personali dei clienti quali:

  - furto di credenziali di autenticazione, di identità elettronica, appropriazione dati di carta di credito.

- **Truffa informatica esterna:** tutti i casi di frodi realizzate da un soggetto esterno all'azienda rivolto a procurare a sé o ad altri un profitto o, comunque, un vantaggio in termini economici, pubblicitari, ideologici/politici, qualora tali frodi causino perdita delle caratteristiche di sicurezza dei dati personali dei soggetti interessati (confidenzialità, integrità o disponibilità) trattati dall'ente/organizzazione o da suoi fornitori. Ad esempio: accesso non autorizzato ed illecito alle basi dati dei sistemi contenenti i dati dei soggetti interessati tramite sfruttamento di vulnerabilità dei sistemi.

- **Truffa informatica interna:** tutti i casi di frodi realizzate da personale interno all'azienda che comportano la violazione dei dati personali. Tali eventi possono derivare dall'utilizzo illecito e/o illegittimo delle informazioni a cui un incaricato del trattamento accede anche se autorizzato.

5.2.3 Eventi Accidentali da trattamenti cartacei

Eventi anomali causati nell'ambito dei trattamenti non automatizzati effettuati su archivi cartacei dei dati personali degli utenti dell'ASL quali:

- **Distruzione accidentale di documenti,** ad esempio:
  - incendio/ allagamento dei locali dove sono presenti archivi cartacei, causati da eventi fortuiti e non dolosi presso le sedi dell'ASL, delle Ditte nominate Responsabili del trattamento dei dati personali, degli outsourcers di archiviazione contratti e dei corrieri per la raccolta dei contratti, delle Ditte per le quali è scaduto il contratto dalle quali si attende la restituzione della documentazione contrattuale;
  - distruzione per errore di documenti originali, senza eventuale copia, da parte di dipendenti interni, di Responsabili, di terzi.

- **Smarrimento di documenti,** ad esempio:
  - perdita di documenti contenenti dati dei cittadini, degli outsourcers (es. archiviazione contratti e dei corrieri per la raccolta dei contratti), ecc.

- **Fornitura involontaria di dati a persona diversa dal contraente**, ad esempio:
  - invio lettera ad Ente senza mandato,
  - gestione ed evasione reclami/richieste di informazioni avanzate da persone diverse dal titolare della linea non delegato,
  - comunicazione di dati dal subentrato al subentrante e viceversa,
  - invio/visualizzazione di fatture a soggetti diversi dal titolare della linea.

5.2.4 Eventi Dolosi da trattamenti cartacei

Comportamenti dolosi da parte di personale interno o soggetti esterni realizzati, attraverso accessi non autorizzati, nell'ambito di trattamenti effettuati su archivi cartacei di dati personali della ASL quali:

- **Distruzione dolosa dei documenti,** ad esempio:
  - incendio doloso provocato da personale interno o soggetti esterni che rende indisponibile in modo definitivo i documenti contenenti dati degli interessati;
  - accesso non autorizzato da parte di terzi ad archivi interni della ASL e distruzione volontaria di documenti contenenti dati degli interessati.
- **Accesso non autorizzato,** ad esempio:
  - accesso non autorizzato da parte di personale interno o soggetti esterni, con lettura e/o copia dei documenti, ad archivi documentali presso le sedi dell'ASL, delle Ditte fornitrici.
- **Furto** da parte di personale interno o soggetti esterni (o non identificati) di documenti cartacei contenenti dati dei soggetti interessati.

6. ATTIVITA' DI MONITORAGGIO

Le attività a tutela della sicurezza dei dati personali trattati dalla Azienda sono svolte, oltre che in occasione di un incidente di sicurezza che potenzialmente potrebbe integrare la fattispecie di violazione dei dati personali, anche attraverso l'ordinaria attività di monitoraggio periodico delle attività di trattamento di cui al Registro dei trattamenti, con particolare attenzione a quei trattamenti valutati a "rischio medio" nella valutazione di impatto e degli eventi che possono arrecare violazioni dei dati, sia digitale ed automatizzata che cartacea

Le attività di monitoraggio si possono suddividere in due tipologie:

- **monitoraggio degli 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 monitorati e gestiti dall'Amministratore di Sistema e/o dalla UOC SIA, responsabile della sicurezza operativa dei sistemi ICT aziendali.

- **monitoraggio dei luoghi fisici** del trattamento e dell'archiviazione di dati personali - I luoghi fisici preposti al trattamento di informazioni personali, con particolare riferimento agli eventuali archivi cartacei, devono essere controllati dagli autorizzati al trattamento (ai vari livelli) e dal responsabile di struttura.

In entrambi i casi, qualora dall'attività di monitoraggio emerga l'evidenza di un incidente di sicurezza con sospetta e/o avvenuta violazione dei dati personali, è obbligatorio da parte o dell'Amministratore di Sistema, del Direttore UOC SIA (prima ipotesi) del Direttore/Responsabile della struttura (seconda ipotesi) informare dell'accaduto il Titolare del trattamento, per il tramite del Responsabile Protezione Dati (DPO) mediante la compilazione dell'Allegato A.

7. SEGNALAZIONE DI INCIDENTI DI SICUREZZA

Le segnalazioni di incidenti di sicurezza relative ai dati personali sono gestite dal Titolare del trattamento, per il tramite del Responsabile della Protezione Dati, con il coordinamento del Responsabile UOSD ROOA.
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.
In ogni caso l'incidente di sicurezza verificatosi, anche se non ha dato luogo a violazione dei dati personali, comporta l'apertura di una scheda di gestione incidente, attivando il processo di analisi, valutazione e individuazione delle misure di miglioramento dell'organizzazione al fine di evitare il ripetersi dell'evento nonché una valutazione delle responsabilità afferenti agli attori coinvolti per attivare le misure compensative del caso. La stessa sarà riportata nel "Registro Incidenti di Sicurezza".

8. MODALITA' OPERATIVA DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

La procedura si compone di 5 fasi, riportata graficamente nel flow chart "Allegato C".

1- Ricezione della segnalazione, rilevazione e registrazione dell'incidente di sicurezza
2- Valutazione preliminare dell'incidente
3 - Valutazione approfondita dell'incidente
4 - Risk assessment e individuazione contromisure.
5 - Notifica all'Autorità Garante e/o comunicazione agli interessati.

8.1 RICEZIONE DELLA SEGNALAZIONE, RILEVAZIONE E REGISTRAZIONE DELL'INCIDENTE DI SICUREZZA

In questa fase si acquisisce la notizia di un incidente di sicurezza, con o senza possibile violazione di dati personali. La segnalazione può pervenire dall'interno o dall'esterno (Responsabili, cittadini). Chiunque appartenente all'organizzazione aziendale riceva la segnalazione dal cittadino inoltrerà la segnalazione al Titolare, secondo la presente procedura.
La segnalazione si effettua compilando, da parte di uno degli attori, l'Allegato "A"ed inviandolo al Titolare per il tramite del RPD.
Il Titolare del trattamento, per il tramite del RPD, effettua la registrazione e l'identificazione univoca della segnalazione su apposito **Registro degli incidenti/data breach.**

8.2 VALUTAZIONE PRELIMINARE DELL'INCIDENTE

In questa fase il Titolare, con il supporto del Responsabile della Protezione Dati, acquisiti dal modello gli elementi utili, avvia una valutazione preliminare dell'incidente al fine di escludere o confermare la sussistenza del Data Breach. Se dall'analisi emergono elementi tali da escludere la possibile violazione di dati personali, l'anomalia viene gestita secondo la procedura standard.
Se, invece, dalla prima analisi emergono estremi di una possibile violazione dei dati personali il Titolare attiva la fase della valutazione approfondita dell'incidente.
Vedi a tal proposito anche "Allegato B" contenente esempi riportati nel documento WP 250 edito dal Gruppo dei Garanti europei ex art.29.

8.3 VALUTAZIONE APPROFONDITA DELL'INCIDENTE

Scopo di questa fase è confermare o meno l'avvenuta violazione di dati personali, di circostanziare in modo completo l'evento e valutare il possibile pregiudizio per i terzi.
Il Titolare, con il supporto del Responsabile Protezione Dati, coinvolto il Responsabile UOSD Rapporto con gli Organi e Organismi Aziendali, per il coordinamento delle varie funzioni aziendali interessate al fine di effettuare una analisi di dettaglio, raccoglie informazioni aggiuntive e valuta il livello di rischio dell'evento e l'eventuale pregiudizio per i terzi.
Detta valutazione sarà effettuata partendo dall'esame delle informazioni riportate nell'Allegato A, aggiungendo tutti gli elementi ulteriori ritenuti necessari ed opportuni.
Se da questa analisi approfondita non si ravviserà l'esistenza di una violazione, l'evento anomalo viene gestito secondo la procedura standard.
Nell'ipotesi in cui, dall'analisi emerga una violazione dei dati personali si configura il DATA BREACH e iniziano a decorrere le 72 ore per effettuare la notifica al Garante.
Dovrà, quindi, essere effettuata tempestivamente la successiva fase al fine di rispettare la vigente normativa in materia.

8.4 RISK ASSESSMENT E INDIVIDUAZIONE DELLE MISURE

Al termine della fase di valutazione approfondita e definizione dell'incidente come data breach, il Titolare del trattamento con il supporto del RPD e, in caso di *violazioni informatiche*, dell'UOC SIA e/o dell'Amministratore di sistema, stabiliranno congiuntamente:

- le opportune misure correttive e di protezione che possano limitare i danni che la violazione causa (*es. 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 adozione delle suddette misure, individuando gli attori e i compiti per limitare la violazione;

- se la violazione ricade nei casi un 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 Titolare, con il supporto del Responsabile delle Protezione dati, nonché delle altre figure coinvolte nell'analisi più approfondita, valuterà la gravità della violazione utilizzando un modello standardizzato, come da Modulo di valutazione del Rischio connesso al Data Breach, secondo le indicazioni di cui all'art. 33 GDPR .
Si precisa che gli obblighi di notifica all'Autorità Garante scaturiscono dal superamento di una soglia di rischio tale da essere *non trascurabile* (*...improbabile che la violazione presenti un rischio... RISCHIO BASSO/MOLTO BASSO*); l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato in caso di un *rischio elevato per i diritti e libertà (RISCHIO* ALTO*)*.

La metodologia adottata nella valutazione dei rischi tiene conto dei due fattori che intervengono in modo fondamentale nella valutazione dei rischi al verificarsi dell'evento "anomalo":

- la **probabilità** che le conseguenze pregiudizievoli si verifichino (P)
- l' **impatto** inteso come gravità del danno che provoca il verificarsi delle conseguenze pregiudizievoli (I)

Infatti dalla combinazione delle due diverse situazioni esistenti rispetto allo specifico trattamento, si ricava la matrice di rischio (R) la cui entità è data dalla relazione

$$\mathbf{R = P \times I}$$

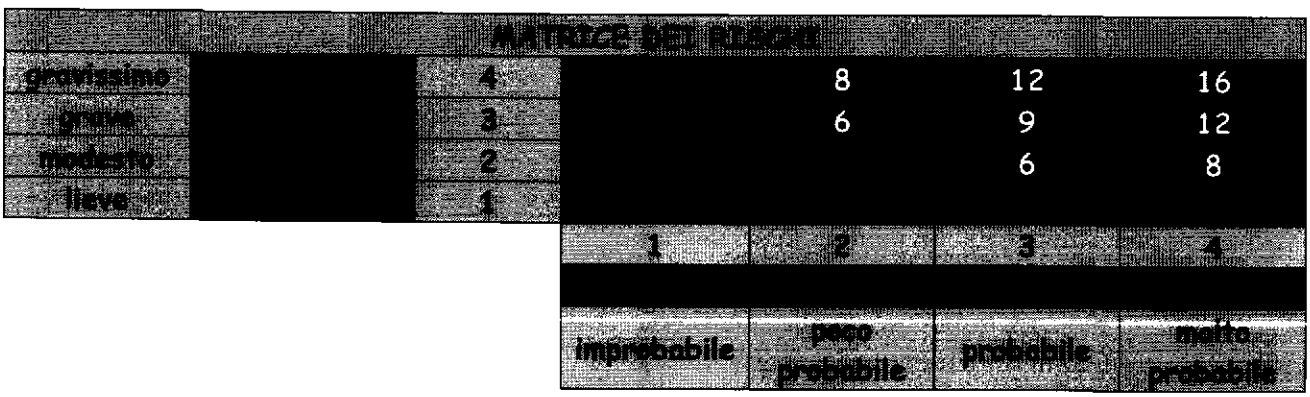
Alla probabilità dell'evento (P) è associato un indice numerico rappresentato nella seguente tabella:

1	improbabile
2	poco probabile
3	probabile
4	molto probabile

Alla gravità del danno (I), stimata analizzandone i sintomi, è associato un indice numerico rappresentato nella seguente tabella:

1	lieve
2	modesto
3	grave
4	gravissimo

La matrice che scaturisce dalla combinazione di **probabilità** ed **impatto** è rappresentata nella figura successiva.



RISCHIO	RANGE
	R=1
	2≤R≤4
Medio	6≤R≤9
Alto	12≤R≤16

Nel caso di specie per lo specifico evento anomalo occorso si considerano 8 sottocategorie di possibili conseguenze pregiudizievoli per l'interessato:

1. Danno per la reputazione V_{f1}
2. Discriminazione V_{f2}
3. Furto d'identità V_{f3}
4. Perdite finanziare V_{f4}
5. Danni fisici o psicologici V_{f5}
6. Perdita di controllo dei dati V_{f6}
7. Altri svantaggi economici o sociali V_{f7}
8. Impossibilità di esercitare diritti, servizi o opportunità V_{f8}

Per poter correlare tutti gli elementi sopradescritti, come normalmente effettuato nelle analisi di "rischio", per ognuno delle sottocategorie di possibili conseguenze è stato stimato il valore (Vf), dato dal prodotto P x I, ricavando rispettivamente: V_{f1} V_{f2} V_{f3} V_{f4} V_{f5} V_{f6} V_{f7} V_{f8}

Per determinare la valutazione totale del rischio si calcola il valore (Mf) ottenuto come * Media aritmetica dei valori Vfi

$$* Mf = \frac{Vf1+Vf2+Vf3+Vf4+Vf5+Vf6+Vf7+Vf8}{8}$$

EVENTO:			
	probabilità (P)	**impatto (I)**	**valutazione dei rischi (R)**
danno per la reputazione			
discriminazione			
furto d'identità			
perdite finanziarie			
danni fisici o psicologici			
perdita di controllo dei dati			
altri svantaggi economici o sociali			
impossibilità esercitare diritti, servizi o opportunità			
		VALUTAZIONE TOTALE	

Il valore così ottenuto viene confrontato con il seguente range per stabilire la gravità della violazione.

	R≤1,99
	2≤R≤5,99
Medio	6≤R≤10,99
Alto	11≤R≤16

8.5. NOTIFICA ALL'AUTORITA' GARANTE E/O COMUNICAZIONE AGLI INTERESSATI

Se la valutazione supera la soglia di 5,99 va effettuata la notifica di data breach all'Autorità Garante. Se si supera la soglia di 11 va effettuata anche la comunicazione agli interessati.

8.5.1 Notifica all'Autorità Garante

Se a seguito delle valutazioni 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 AV, per il tramite del Responsabile Protezione Dati, provvederà alla notifica all'Autorità Garante senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui è stata accertata la "violazione dei dati personali".

Pertanto:

- senza ingiustificato ritardo, entro le 72 ore dall'accertamento, il Titolare, per il tramite del RPD, trasmetterà, tramite pec sottoscritta digitalmente all'Autorità Garante, tutte le informazioni disponibili relative al data breach e, comunque, quelle indicate nell'art. 33 del Regolamento, ed archivia la notifica e le relative evidenze (v. infra);
- se la notifica avviene oltre le 72 ore dall'accertamento deve essere corredata dai motivi del ritardo;
- se la prima notifica avvenuta entro le 72 ore dalla segnalazione non è completa (es. violazioni molto complesse) la stessa deve essere successivamente integrata, con la massima sollecitudine, specificando i motivi del ritardo (art. 33 par. 1)

L'articolo 33, paragrafo 3 del Regolamento stabilisce che la notifica deve contenere almeno i seguenti elementi:

- a) descrizione della natura della violazione dei dati personali compresi, ove possibile, delle categorie e del numero approssimativo di interessati in questione nonché delle categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- b) comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- c) descrizione delle probabili conseguenze della violazione dei dati personali;
- d) 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 anche, se del caso, per attenuarne i possibili effetti negativi".

Atteso che il l'Autorità Garante ha preannunziato la definizione di un modello da utilizzare in tali fattispecie, allo stato non ancora definito, fino a tale data la notifica sarà effettuata via pec con comunicazione firmata digitalmente dal legale rappresentante al seguente indirizzo: protocollo@pec.gpdp.it.
Non appena sarà disponibile il modello definito dall'Autorità Garante lo stesso entrerà automaticamente in uso rispettando anche eventuali istruzioni emanate a corredo dello stesso.

8.5.2 Comunicazione agli interessati

Se a seguito della valutazione e del risk assessment effettuato nel rispetto della presente procedura, è stata valutata la necessità di effettuare la comunicazione della violazione dei dati a coloro dei cui dati si tratta, 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 del Responsabile Protezione Dati, provvederà alla comunicazione all'Interessato senza ingiustificato ritardo.
Quanto al contenuto di tale comunicazione, il Titolare del trattamento dovrà:
• comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
• descrivere le probabili conseguenze della violazione dei dati personali;
• 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, 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, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.
Nel caso in cui la comunicazione dovesse pregiudicare lo svolgimento delle verifiche sull'evento data breach il RPD può chiedere all'Autorità Garante l'autorizzazione a ritardare la citata comunicazione per il tempo necessario all'espletamento di tali verifiche.

9 REGISTRO INCIDENTI /DATA BREACH

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente di sicurezza dei dati la ASL AV sarà tenuta a conservare tutta la documentazione inerente.
A tal fine il Responsabile della Protezione Dati provvede alla tenuta di un apposito Registro degli Incidenti/Data Breach, in cui sono riportate le seguenti informazioni:

- identificativo incidente;
- data incidente;
- data segnalazione incidente
- descrizione della natura dell'incidente;
- categoria di interessati e del numero approssimativo;
- categoria di dati personali coinvolti e il numero approssimativo di registrazioni dei dati personali in questione;
- valutazione dell'incidente (violazione -data breach- o quasi violazione –near miss-);
- conseguenze dell' incidente;
- misure adottate per incidente. Nel caso di violazione dei dati personali 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 anche, se del caso, per attenuarne i possibili effetti negativi;

- notifica all'Autorità Garante Privacy (protocollo e data)
- nel caso di ritardo/incompletezza della notifica esplicazione dei motivi e data dell'integrazione delle notizie mancanti
- comunicazione agli interessati (data e modalità).

Il Registro sarà continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.

Il Registro degli incidenti conterrà, quindi, sia le "quasi violazioni" sia le "violazioni dei dati personali" accertate. Dall'analisi delle quasi violazioni si potranno apportare le azioni di miglioramento finalizzate, comunque, ad abbassare il livello di rischio del verificarsi della violazione vera e propria.

Detta procedura standard è rappresentata nell'allegata flow chart "Allegato C" nell'ambito della fase 5.

Il Responsabile UOSD Rapporti con
Organi e Organismi aziendali
Dr.ssa Alessandra Antocicco

Il Responsabile Protezione Dati
Dr.ssa Marisa Prudente

Prot.n._____ del _____

ALLEGATO "A"

Al Direttore Generale/Titolare del Trattamento
per il tramite del DPO
rpd.privacy@pec.aslavellino.it
oppure
responsabileprotezionedati@aslavellino.it

Oggetto: Segnalazione incidente di sicurezza

Data scoperta:

Data dell'incidente:

- o il _____
- o tra il _____ e il _____
- o in un tempo non ancora determinato
- o è possibile che sia ancora in corso

Nome della persona che ha riferito della violazione e suoi dati di contatto (mail - telefono):

Denominazione della/e banca/banche dati, archivio/archivi (cartacei e/o informatici), documento/i oggetto di presunta violazione dei dati personali ivi trattati e breve descrizione dell'accaduto (sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione):

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Dati oggetto di violazione?

- o Dati anagrafici/codice fiscale
- o Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)
- o Dati relativi a minori
- o Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- o Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- o Dati giudiziari
- o Copia per immagine su supporto informatico di documenti analogici

- Ancora sconosciuto
- Altro :

Dispositivo oggetto della violazione

- Computer
- Rete
- Dispositivo mobile
- File o parte di un file
- Strumento di *backup*
- Documento cartaceo
- Altro :

Tipo di violazione

- Lettura (presumibilmente i dati non sono stati copiati)
- Copia (i dati sono ancora presenti sui sistemi del titolare)
- Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- Altro :

Categorie e Numero approssimativo di interessati coinvolti nella violazione dei dati personali trattati nell'ambito della banca dati

CATEGORIA (specificare): _____

- N° ____ persone
- Circa n° ____ persone
- Un numero (ancora) sconosciuto di persone

Misure tecniche e organizzative già applicate ai dati oggetto di violazione (specificare):

Azioni poste in essere al momento della scoperta della presunta violazione per contenere la violazione dei dati e prevenire simili violazioni future (specificare):

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del segnalante)

- Basso/trascurabile
- Medio
- Alto
- Molto alto

Il Direttore/Responsabile
UO interessata
(firma)

ALLEGATO "B"

Casi pratici di sussistenza o meno di un Data Breach
(Esempi riportati nel documento WP 250 edito dal Gruppo dei Garanti europei ex art.29)

Esempio 1
Viene effettuato un back up di un archivio di dati personali su una chiavetta USB criptata. La chiavetta viene rubata.
Notifica della data breach al Garante?
NO
Notifica della data breach all'interessato?
NO
Note/Raccomandazioni
Nella misura in cui: (1) è stata utilizzata una tecnologia crittografica basata su algoritmi aggiornati e sicuri in base allo stato dell'arte; (2) esistono altri back up dell'archivio su altri supporti; (3) la chiavetta USB non è stata compromessa; (4) può essere comunque effettuato in tempo utile un *restore* dei dati personali, l'evento **non** rappresenta una ipotesi di *data breach* da notificare. Tuttavia, se successivamente si verifica una compromissione della chiavetta o dell'algoritmo di crittografia, tale ipotesi comporterà l'obbligo di notifica.

Esempio 2
Un Titolare del trattamento gestisce un servizio on line agli utenti. A seguito di un attacco hacker contro tale servizio, i dati degli utenti vengono diffusi. Il gestore di questo servizio ha clienti in un solo Stato membro.
Notifica al Garante?
SI, poiché vi è un probabile rischio per i diritti e le libertà degli interessati (gli utenti del servizio i cui dati sono diffusi a seguito dell'attacco).
Notifica all'interessato?
SI, laddove vi sia un rischio elevato per i diritti e le libertà degli interessati (gli utenti del servizio i cui dati sono diffusi a seguito dell'attacco), in base alla natura dei dati oggetto dell'attacco e alle conseguenze.

Esempio 3
Una temporanea interruzione di corrente elettrica causa l'impossibilità di resa dei servizi da parte di un call center gestito da un Titolare del trattamento. Gli utenti non sono in grado di chiamare il call center né di accedere ai propri records.
Notifica della data breach al Garante?
NO
Notifica della data breach all'interessato?
NO
Note/Raccomandazioni
Anche se tale incidente non è soggetto a nessuna notifica, resta l'obbligo per il Titolare del trattamento di riportare, descrivere e conservare i riferimenti all'incidente nell'Inventario Incidenti di cui all'art. 33, comma 5 del GDPR.

Esempio 4
Un Titolare del trattamento subisce un attacco di tipo ransomware che determina il blocco e la crittografia di tutti i suoi dati sui sistemi. Non sono disponibili back-up e i dati non possono dunque essere ripristinati. Dopo le opportune verifiche e investigazioni, risulta che lo scopo del ransomware è esclusivamente quello di crittografare i dati e che nessun malware è presente nei sistemi del Titolare del trattamento.
Notifica della data breach al Garante?
SI, in quanto vi è una data breach rappresentata da una perdita di disponibilità dei dati personali che impatta sugli interessati.
Notifica della data breach all'interessato?
SI, in quanto vi è una data breach rappresentata da una perdita di disponibilità dei dati personali che impatta sugli interessati. Vi potrebbero essere altresì anche altre conseguenze in base alla natura dei dati personali.
Note/Raccomandazioni
Ove fossero stati disponibili back up e fosse stato possibile ripristinare i dati personali in breve tempo, tale incidente non avrebbe comportato l'obbligo di notifica della violazione né all'Autorità né agli interessati poiché non vi sarebbe stata perdita permanente di disponibilità dei dati medesimi né di confidenzialità (data la

crittografia). In tali casi, ove non fosse stato notificato all'Autorità l'incidente, comunque l'Autorità avrebbe potuto – ove ne fosse venuta a conoscenza – avviare una indagine presso il Titolare per verificare la conformità delle misure di sicurezza da questi adottate all'articolo 32 GDPR.

Esempio 5

Il cliente di una banca chiama la sua agenzia per informarla di un data breach: dichiara di aver ricevuto l'estratto conto mensile di un altro correntista. Nelle 24 ore successive la banca effettua gli accertamenti del caso e stabilisce che molto probabilmente si è verificata una violazione di dati personali e se tale incidente è sistemico e può interessare anche altri clienti della banca.

Notifica della data breach al Garante?

SI.

Notifica della data breach all'interessato?

SI, ma solo agli interessati effettivamente coinvolti, non anche agli altri che potrebbero essere coinvolti.

Note/Raccomandazioni

Se dopo le prime investigazioni emerge che sono coinvolti anche altri clienti della banca, il Titolare del trattamento dovrà integrare la notifica di violazione già svolta all'Autorità con le ulteriori informazioni e dovrà notificare anche agli interessati.

Esempio 6

Il gestore di un marketplace on line, con clienti di diversi Stati europei, è vittima di un cyber attacco a seguito del quale usernames, passwords e storico degli acquisiti della clientela sono pubblicati on line.

Notifica della data breach al Garante?

SI. Nel caso siano coinvolte più autorità privacy – data la natura cross-border della violazione dei dati personali – andrà effettuata la notifica della violazione alla leading Authority (individuabile in base alle)

Notifica della data breach all'interessato?

SI, poiché è elevato il rischio per i diritti e le libertà dei clienti coinvolti.

Note/Raccomandazioni

Il gestore del marketplace dovrebbe prendere immediate misure volte a mitigare il rischio. Ad esempio forzando il reset delle password dei clienti.

Esempio 6

Il fornitore di servizi di hosting per siti web che agisce quale Responsabile esterno del trattamento si avvede di un errore nel codice di controllo delle autorizzazioni a seguito del quale qualsiasi utente può accedere all'account di qualsiasi altro utente.

Notifica della data breach al Garante?

Come Responsabile esterno del trattamento e fornitore dei servizi di hosting ai suoi clienti (i Titolari del trattamento), la società di hosting deve immediatamente informare e senza ritardo della violazione i suoi clienti (i Titolari del trattamento). Assumendo che la società di hosting abbia condotto le propri investigazioni, nel momento in cui i Titolari sono informati dal Responsabile esterno, è questo il momento in cui essi diventano consapevoli della violazione e dunque da tale momento decorre il termine di 72 ore per effettuare la notifica all'Autorità.

Notifica della data breach all'interessato?

Se non vi è un rischio elevato, non vi è obbligo di notificare la violazione agli interessati.

Note/Raccomandazioni

Esempio 7

Per errore di un addetto del Titolare del trattamento le schede anagrafiche dei partecipanti a un corso di formazione sono trasmesse ad una mailing list errata di più di mille destinatari.

Notifica della data breach al Garante?

SI.

Notifica della data breach all'interessato?

SI. Va comunque valutato il livello di gravità la severità delle conseguenze dell'errato invio.

Note/Raccomandazioni: ---------

Esempio 8

Una email di direct marketing è inviata in copia palese e non nascosta a molti destinatari, che dunque possono vedere i recapiti di posta elettronica di ciascun destinatario in copia..

Notifica della data breach al Garante?

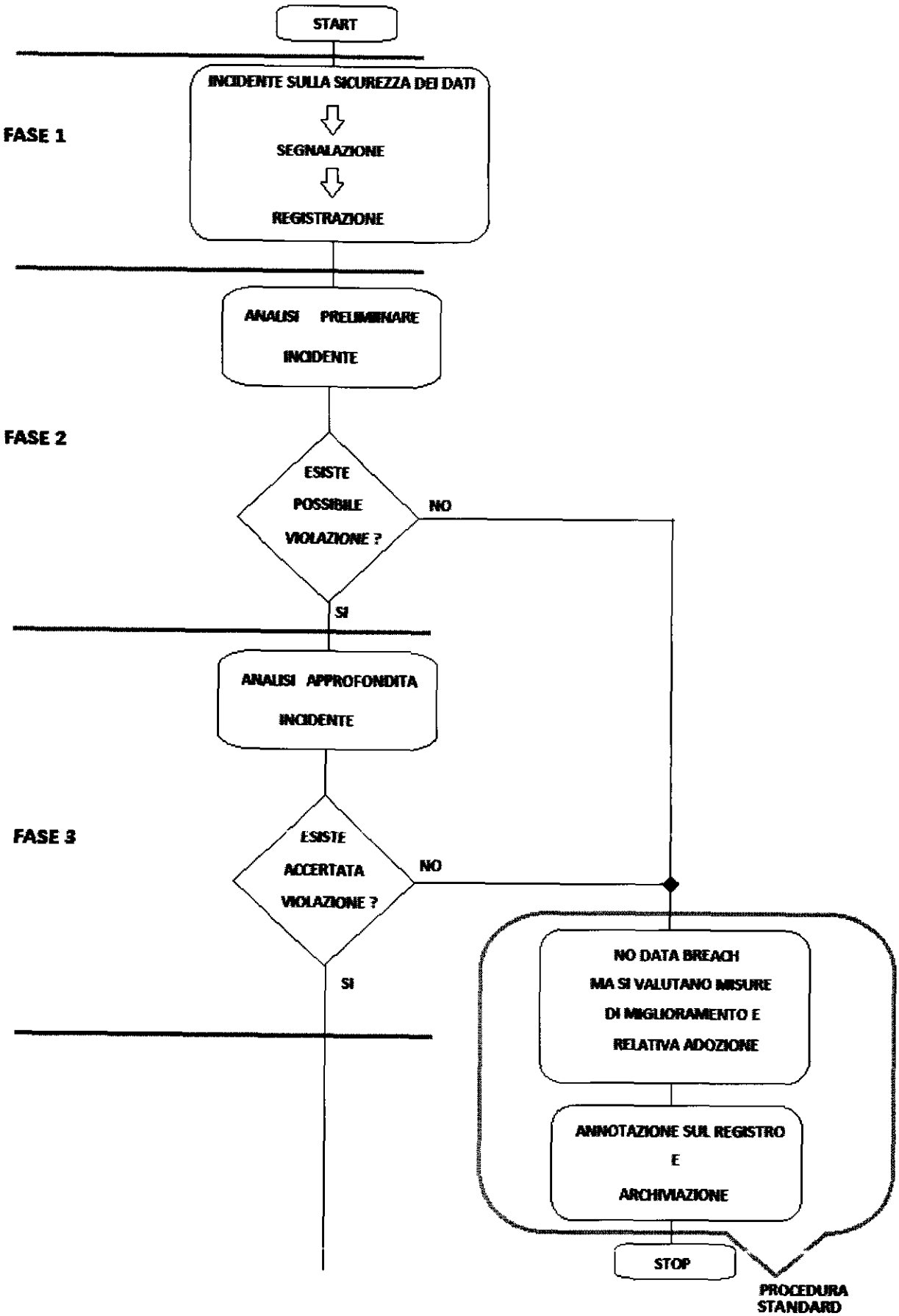
SI, ma solo nel caso in cui sia coinvolto un elevato numero di interessati, vi sia una natura delicata (es: la mailing list dei pazienti di uno studio medico) o il contenuto del messaggio sia rischioso (es: invio del primo pin o password per accedere a un servizio).

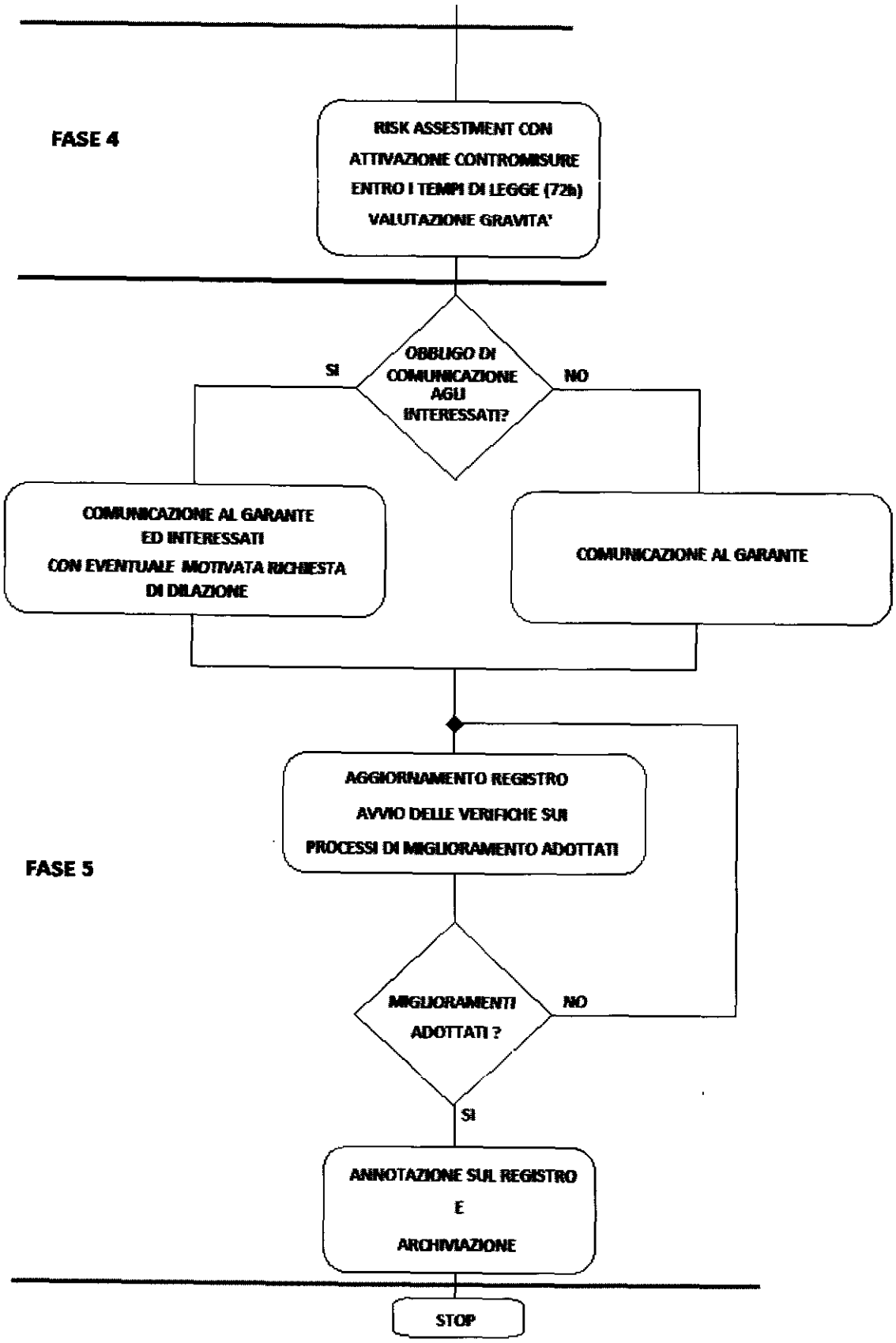
Notifica della data breach all'interessato?

SI. Va comunque valutato il livello di gravità la severità delle conseguenze dell'errato invio.

Note/Raccomandazioni

Potrebbe non esservi alcun obbligo di notifica, né all'Autorità né agli interessati, ove sia molto limitato il numero di interessati coinvolti e la natura dei dati sia ordinaria e non
delicata.


START
INCIDENTE SULLA SICUREZZA DEI DATI
SEGNALAZIONE
REGISTRAZIONE
FASE 1
ANALISI PRELIMINARE
INCIDENTE
FASE 2
ESISTE
POSSIBILE
VIOLAZIONE ?
NO
SI
ANALISI APPROFONDITA
INCIDENTE
FASE 3
ESISTE
ACCERTATA
VIOLAZIONE ?
NO
SI
NO DATA BREACH
MA SI VALUTANO MISURE
DI MIGLIORAMENTO E
RELATIVA ADOZIONE
ANNOTAZIONE SUL REGISTRO
E
ARCHIVIAZIONE
STOP
PROCEDURA
STANDARD


FASE 4
RISK ASSESTMENT CON
ATTIVAZIONE CONTROMISURE
ENTRO I TEMPI DI LEGGE (72h)
VALUTAZIONE GRAVITA'
OBBLIGO DI
COMUNICAZIONE
AGLI
INTERESSATI?
SI
NO
COMUNICAZIONE AL GARANTE
ED INTERESSATI
CON EVENTUALE MOTIVATA RICHIESTA
DI DILAZIONE
COMUNICAZIONE AL GARANTE
FASE 5
AGGIORNAMENTO REGISTRO
AVVIO DELLE VERIFICHE SUI
PROCESSI DI MIGLIORAMENTO ADOTTATI
MIGLIORAMENTI
ADOTTATI ?
NO
SI
ANNOTAZIONE SUL REGISTRO
E
ARCHIVIAZIONE
STOP

☐ Esecutiva in data _____

INVIO AL COLLEGIO SINDACALE

Prot. n. 312 *del* 26 MAR. 2019

Il Responsabile Ufficio
Delibere e Determine