AZIENDA SANITARIA LOCALE "NO" - NOVARA
Viale Roma, 7 - NOVARA

DELIBERAZIONE

DEL DIRETTORE GENERALE

Numero 364 *Data* - 2 OTT. 2019

PROPOSTA ISTRUTTORIA DEL DIRETTORE GENERALE n° 81

OGGETTO: *REGOLAMENTO UE 679/2016, ARTT. 33 E 34 – VIOLAZIONE DATI PERSONALE (DATA BREACH) - PROCEDURA*

§§§§§§§§§§

IL DIRETTORE GENERALE
(nominato con d.G.R. n° 11-6930 del 29 maggio 2018)

Nella data sopraindicata, su propria iniziativa istruttoria - previa acquisizione del parere dei Direttori: Amministrativo e Sanitario - ha assunto, in Novara, presso la sede dell'Ente, la deliberazione di cui all'interno.

DELIBERAZIONE N° 364 **IN DATA** - 2 OTT. 2019

*

*

OGGETTO: ***REGOLAMENTO UE 679/2016, ARTT. 33 E 34 – VIOLAZIONE DATI PERSONALE (DATA BREACH) - PROCEDURA***

* *

IL DIRETTORE GENERALE

RICHIAMATO il Regolamento UE 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), ed in particolare, per la parte che qui rileva:

- art. 33: "*Notifica di una violazione dei dati personali all'autorità di controllo*";
- art. 34: "*Comunicazione di una violazione dei dati personali all'interessato*";

il d. Lgs. 30 giugno 2003, n° 196, nel testo novellato dal d. Lgs. 10 agosto 2018, n° 101: "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

CONSIDERATO che per "violazione dei dati personali" (data breach) si intende, ai sensi della vigente normativa, una "*violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, che possa compromettere la riservatezza, l'integrità o la disponibilità di dati personali*";

RICHIAMATE le Linee Guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679, nella versione emendata ed adottata in data 6 febbraio 2018 dal Gruppo di lavoro istituito in virtù dell'articolo 29 della direttiva 95/46/CE quale organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata e con i compiti fissati dall'articolo 30 della direttiva 95/46/CE e dall'articolo 15 della direttiva 2002/58/CE;

VISTO il Provvedimento del Garante per la Protezione dei Dati Personali in data 30 luglio 2019 (n° 9126951) con il quale viene approvato il (nuovo) modello di notifica all'Autorità Garante, modello che si ritiene di adottare in allegato all'emananda procedura;

RITENUTO opportuno e necessario dotare l'ASL NO di una procedura, elaborata e condivisa con il DPO aziendale, nominato con deliberazione n° 103 del 23 maggio 2018, nonché dall'Unità Supporto Privacy aziendale, nominata con deliberazione n° 253 del 23 novembre 2018, nel testo allegato quale parte integrante e sostanziale al presente provvedimento;

con il concorso dei pareri dei Direttori: Amministrativo e Sanitario, pareri inseriti nel presente provvedimento.

D E L I B E R A

per le motivazioni e con i criteri di cui in premessa,

1.) **di approvare** la procedura aziendale "Gestione delle violazioni di dati personali (data breach)", allegata quale parte integrante e sostanziale al presente provvedimento;

2.) **di depositare** copia della procedura di cui al precedente punto 1.) presso la SSD Governo Clinico e Sviluppo Strategico, che ne curerà l'archiviazione nel data base delle procedure/percorsi assistenziali;

3.) **di dare mandato** al Direttore della s.c. Affari Istituzionali, Legali, Comunicazione, Anticorruzione e Trasparenza di provvedere alla distribuzione del documento come previsto dalla deliberazione n° 109/2018;

4.) **di dare atto** che il presente provvedimento non comporta alcun onere di spesa a carico della deliberante Amministrazione.

LETTO, APPROVATO E SOTTOSCRITTO

IL DIRETTORE GENERALE
(Dott.ssa Arabella FONTANA)

Istruttoria e stesura dattilografica: Dott. Claudia Teruggi

REGIONE PIEMONTE A.S.L. NO AZIENDA REGIONALE

SEGUE DELIBERAZIONE N. 364 *IN DATA* - 2 OTT. 2019

PARERI DEI DIRETTORI AMMINISTRATIVO E SANITARIO

VISTO *l'art. 3, d. Lgs. 30 dicembre 1992, n° 502, e successive modificazioni ed integrazioni*;

VALUTATA la proposta di atto deliberativo ad istruttoria del ***Direttore Generale*** ed iscritta al n° **81** dell'apposito registro, di cui il presente parere costituisce allegato;

I DIRETTORI: AMMINISTRATIVO E SANITARIO

ognuno per la rispettiva competenza

ESPRIMONO PARERE FAVOREVOLE

il Direttore Amministrativo: *dott. Francesco Arena*

il Direttore Sanitario: *dott.ssa Elide Azzan*

REGIONE PIEMONTE A.S.L. NO AZIENDA REGIONALE

ALLEGATO

AL PROVVEDIMENTO R.G. N° 364 IN DATA - 2 OTT. 2019

COMPOSTO DA N. TRENTOTTO FACCIATE

REGIONE PIEMONTE
A.S.L. NO
AZIENDA REGIONALE

364 - 2 OTT. 2019

	ASLNO	CODICE: 012/ASLNO/19/Rev.0 IN APPLICAZIONE DAL: 02/10/2019 PAG. 12

PROCEDURA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI "DATA BREACH"

REVISIONE

Rev.	MOTIVO	MODIFICHE APPORTATE	Data

REDATTO	VERIFICATO	APPROVATO
Dott. Claudio Teruggi Direttore S.C. Affari Istituzionali, Legali, Comunicazione, Anticorruzione e Trasparenza Dott.ssa Luisella Cendron Direttore S.C. Servizio Informativo e Controllo di Gestione Dott.ssa Lucia Paola Zanetta Responsabile S.S. Coordinamento Amministrativo Ospedaliero e Libera Professione	Dott.ssa Daniela Sarasino Dirigente Responsabile S.s.d. Governo Clinico e Sviluppo Strategico	Dott.ssa Arabella Fontana Direttore Generale
Data: 19/09/2019	Data: 02/10/2019	Data: 02/10/2019

INDICE

1.PREMESSA

Il Regolamento UE 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla "protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (Regolamento Generale sulla Protezione dei Dati Personali), prevede all'art. 33 e all'art. 34 la gestione dei casi di violazione dei dati personali ("Data Breach").

2. SCOPO/OBIETTIVO

La presente procedura sulla gestione delle violazioni di dati personali ("Data Breach") ha lo scopo di descrivere il processo da seguire nel caso in cui si verifichi una violazione (reale o sospetta) dei dati personali. Il processo di gestione definisce altresì le modalità con cui l'Azienda mantiene traccia delle attività svolte e dei risultati ottenuti. Le registrazioni di tali eventi sono una collezione coerente e strutturata di dati che dimostra l'effettiva ed efficace applicazione del Sistema di Gestione per la Privacy (SGP).

3. CAMPO DI APPLICAZIONE

La presente Procedura si applica all'Ente ASL di Novara, in qualità di Titolare del Trattamento dei dati personali, nei casi in cui si verifichi, in ordine alle attività di trattamento dei dati personali, una violazione o una sospetta violazione.

4. ABBREVIAZIONI

- **AILCAT**: Affari Istituzionali, Legali, Comunicazione, Anticorruzione e Trasparenza;
- **DG**: Direttore Generale ASL;
- **DMPO**: Direzione Medica Presidio Ospedaliero;
- **DPO:** Data Protection Officer;
- **RPD:** Responsabile Protezione Dati
- **GDPR**: Regolamento Generale sulla Protezione dei Dati Personali (UE) 2016/679;
- **SICG**: Servizio Informativo e Controllo di Getsione;
- SGP: Sistema Gestione Privacy;
- **VD**: Vertice Direzionale;
- **USP**: Unità di Supporto Privacy.

5. DEFINIZIONI

- **Autorità di Controllo**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR. In Italia Autorità Garante Protezione Dati Personali.
- **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.
- **Interessato al trattamento**: è la persona fisica cui si riferiscono i dati personali oggetto di trattamento.

- **DPO/RPD**: è una persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37.1 del GDPR dal Titolare o dal Responsabile del Trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR.
- **Titolare del Trattamento o Titolare**: 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 o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
- **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.
- **Responsabile del Trattamento o Responsabile**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'Interessato.
- **Persona Autorizzata**: si tratta dei Collaboratori autorizzati al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del GDPR.
- **Violazione dei Dati Personali (Data Breach)**: è 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.
- **Unità di Supporto Privacy (USP):** gruppo di lavoro aziendale costituto con delibera n. 253/2018 del 23.11.2018 con il compito di relazionarsi con la Direzione Generale e con il team del DPO per fornire indicazioni tecniche, per la propria area di competenza, nonché il supporto operativo connesso all'attuazione della normativa e all'individuazione più appropriata delle scelte decisionali e strategiche che la disciplina in ambito di trattamento dei dati personali richiede.

6. CRITERI DI INCLUSIONE/ESCLUSIONE

Non applicabile.

7. MODALITÀ OPERATIVE

7.1 FASE 1: Raccolta delle informazioni

L'evento scatenante del processo è la segnalazione che può pervenire da diversi canali:
Canali interni:

- Attori coinvolti nel Sistema di Gestione Privacy (Titolare, Responsabile, personale autorizzato al Trattamento);
- Personale dell'ASL di Novara;
- DPO/RPD.

Canali esterni:
Le segnalazioni possono, altresì, pervenire da fonti esterne o dall'analisi di informazioni presenti sul Web, ovvero dai Responsabili esterni.

Inoltre, ogni Interessato può segnalare, anche solo in caso di sospetto, che i propri Dati Personali siano stati utilizzati abusivamente o fraudolentemente da un terzo. In tal caso, l'Interessato può richiedere all'azienda la verifica dell'eventuale Violazione.

MODALITÀ DI COMUNICAZIONE
Le segnalazioni, a qualunque soggetto/funzione pervengano, devono essere tempestivamente comunicate al Titolare e al RPD/DPO non oltre 12/24 ore dalla conoscenza della Violazione, ove possibile a mezzo PEC, al seguente indirizzo pec: protocollogenerale@pec.asl.novara.it, e al seguente indirizzo di posta elettronica: rpd@asl.novara.it
La presa in carico di tutte le segnalazioni è di responsabilità dell'Unità di Supporto Privacy, designato dal Titolare che provvederà a gestirle coinvolgendo le altre funzioni interessate secondo quanto specificato nella presente Procedura.

7.2 FASE 2: ANALISI DELLE SEGNALAZIONI

ANALISI PRELIMINARE ED ELABORAZIONE DELLA SCHEDA EVENTO
L'USP o suo referente avvia un'analisi preliminare finalizzata alla raccolta dei Dati concernenti l'anomalia ed alla compilazione della Scheda Evento *(Cfr. Cod: 026/Mod/19/Rev.n)* allegata alla presente Procedura e contenente tutte le informazioni raccolte:

- Data evento anomalo;
- Data presunta di avvenuta Violazione;
- Data ed ora in cui si è avuta conoscenza della Violazione;
- Fonte della segnalazione;
- Tipologia della Violazione e delle informazioni coinvolte;
- Descrizione evento anomalo;
- Numero Interessati coinvolti;
- Numerosità di Dati Personali di cui si presume una Violazione;
- Indicazione del luogo in cui è avvenuta la Violazione dei Dati, specificando la circostanza (ad esempio: smarrimento di Device Mobili, etc.);
- Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei Dati coinvolti, con indicazione della loro ubicazione.

La Scheda Evento viene, quindi, destinata all'analisi di primo livello descritta di seguito.

ANALISI DI PRIMO LIVELLO - VERIFICA DELLA SEGNALAZIONE
Obiettivo dell'analisi di primo livello è quella di verificare che la segnalazione non riguardi un cd. "falso positivo".
Nel caso in cui la Violazione relativa ai Dati Personali sia accertata, l'USP, responsabile dell'analisi di primo livello, con la collaborazione delle aree coinvolte dalla Violazione, recupera le informazioni di dettaglio sull'evento, funzionali alle analisi di secondo livello, e le riporta nella Scheda Evento.
Nel caso in cui l'evento segnalato risulti essere un "falso positivo", si chiude l'incidente e la funzione Sistemi Informativi (IT/Security), supportata dalle altre funzioni interne al gruppo privacy, si attiva per effettuare un raffinamento delle regole di rilevazione dei falsi positivi, comunicando via e-mail l'esito dell'analisi all'USP.

L'evento viene comunque inserito a cura della Struttura AILCAT nel Registro dei "Data Breach" (Cfr.Cod :024/Mod/19/Rev.n) in allegato alla presente Procedura, nell'apposita sezione dedicata agli "eventi falsi positivi".

ANALISI DI SECONDO LIVELLO - SCHEDA VIOLAZIONE DATI

Per l'analisi di secondo livello è convocata l'USP, supportata e messa in contatto, tramite i diversi mezzi di comunicazione disponibili (telefono, e-mail, ...), con le seguenti strutture aziendali:

- DIRETTORE GENERALE;
- DIREZIONE AMMINISTRATIVA;
- DIREZIONE SANITARIA;
- SISTEMI INFORMATIVI (IT/SECURITY);
- DPO/RPD;
- AFFARI GENERALI E LEGALI;
- DIRETTORI/RESPONSABILI DELLE STRUTTURE COINVOLTE;
- ALTRI SOGGETTI INTERNI e/o ESTERNI individuati per la specifica violazione.

In tutti i casi, si procede ad analizzare congiuntamente tutte le informazioni raccolte e a redigere una Scheda Violazione Dati *(Cfr. Cod: 025/Mod/19/Rev.n)* allegata alla presente Procedura, per le conseguenti valutazioni.

In particolare, l'evento viene classificato tra i seguenti casi:

- Distruzione di Dati illecita;
- Perdita di Dati illecita;
- Modifica di Dati illecita;
- Distruzione di Dati accidentale;
- Perdita di Dati accidentale;
- Modifica di Dati accidentale;
- Divulgazione di Dati non autorizzata;
- Accesso ai Dati Personali illecito.

La Violazione deve essere valutata secondo i livelli di rischio:

- BASSO;
- MEDIO;
- ALTO.

Il rischio è riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche, anche diverse dall'Interessato, a cui si riferiscono i Dati, a causa della Violazione dei Dati Personali:

- Discriminazioni;
- Furto o usurpazione d'identità;
- Perdite finanziarie;
- Pregiudizio alla reputazione;
- Perdita di riservatezza dei Dati Personali protetti da segreto professionale;
- Decifratura non autorizzata della pseudonimizzazione;
- Danno economico o sociale significativo;
- Privazione o limitazione di diritti o libertà;
- Impedito controllo sui Dati Personali all'Interessato;
- Danni fisici, materiali o immateriali alle persone fisiche.

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

- 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, Dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;

- 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;
- Che si tratti di Dati di persone fisiche vulnerabili, in particolare minori;
- Che il Trattamento riguardi una notevole quantità di Dati Personali;
- Che il Trattamento riguardi un vasto numero di Interessati.

L'USP deve provvedere affinché siano tempestivamente adottate misure che consentano di minimizzare le conseguenze negative della Violazione.

7.3 FASE 3: NOTIFICA E COMUNICAZIONE

NOTIFICA ALLA AUTORITÀ DI CONTROLLO

Redatta la Scheda Violazione Dati, l'USP deve valutare le azioni da intraprendere ed avviare la notifica all'Autorità di Controllo e, ove necessario, la comunicazione agli Interessati, verificando e validando la documentazione pervenuta dalle precedenti fasi di lavoro.

Il Titolare notifica la Violazione all'Autorità di Controllo competente 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, va corredata dei motivi del ritardo.
Con Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [9126951] è stato definito il modello da utilizzare ed inviare tramite PEC.
La versione in vigore al momento di stesura della presente procedura è reperibile al link:
https://www.gpdp.it/documents/10160/0/Modello+notifica+Data+Breach.pdf/6d1fa433-88dc-2711-22ab-dd5d476abe74?version=1.1).

COMUNICAZIONE DELLA VIOLAZIONE ALL'INTERESSATO

Laddove la Violazione presenti un rischio per i diritti e le libertà delle persone fisiche, il Titolare, con la collaborazione dell'USP ed in particolare della Struttura AILCAT, deve informare gli Interessati dell'evento anomalo, a norma degli artt. 33-34 del GDPR. La comunicazione dovrà avere luogo nei casi in cui la Violazione presenti rischi classificati come "ALTI" nella Scheda Violazione Dati *(Cfr. Cod:025/Mod/19/Rev.n)* allegata alla presente Procedura.

La comunicazione deve essere rivolta all'Interessato senza ingiustificato ritardo dall'avvenuta conoscenza e valutazione della Violazione, attraverso il canale di comunicazione ritenuto più idoneo; deve essere intellegibile, concisa, trasparente e facilmente accessibile; deve essere utilizzato un linguaggio semplice e chiaro, adottando, se possibile, la stessa lingua parlata dall'Interessato.

La comunicazione di "Data Breach" all'Interessato deve contenere le seguenti informazioni:

- Data ed ora della Violazione (anche solo presunta) e data ed ora in cui si è avuto conoscenza della stessa;
- La natura della Violazione dei Dati Personali;
- Il nome ed i Dati di contatto del soggetto presso cui ottenere più informazioni;
- Le probabili conseguenze della Violazione dei Dati Personali;

- La descrizione delle misure adottate o di cui si propone l'adozione da parte dell'Ente per porre rimedio alla Violazione dei Dati Personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Deve essere valutata l'opportunità o meno di comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

- Sono state messe in atto le misure tecniche ed organizzative adeguate di protezione e, tali misure erano state applicate ai Dati Personali oggetto della Violazione, in particolare, quelle destinate a rendere i Dati Personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; salvo i casi in cui la Violazione della sicurezza ha comportato la distruzione o la perdita dei Dati Personali degli Interessati;
- Sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà delle persone fisiche; in tal caso, è necessario documentare le misure nella Scheda di Violazione;
- Detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede, invece, ad una comunicazione pubblica o ad una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia.

Si riporta il Modello di comunicazione all'Interessato della Violazione dei Dati Personali *(Cfr. Cod: 027/Mod/19/rev.n).*

7.4 FASE 4: REGISTRAZIONE SEGNALAZIONE NEL REGISTRO DEI "DATA BREACH"

Nel Registro dei "Data Breach" (Cfr.Cod.024/Mod/19/Rev.n), allegato alla presente Procedura, il Titolare documenta ogni singolo evento, sia esso, FALSO, IRRILEVANTE ovvero RILEVANTE; in quest'ultimi due casi, devono essere indicate nel Registro:

- Le conseguenze del Data Breach;
- I provvedimenti adottati per porvi rimedio o attenuarne le conseguenze;
- L'eventuale notificazione all'Autorità di Controllo;
- L'eventuale comunicazione all'Interessato.

Tale documentazione consente all'Autorità di Controllo di verificare il rispetto delle norme in materia di notificazione delle Violazioni di Dati Personali.

Il Registro dei "Data Breach" è tenuto a cura del Titolare o del Responsabile del Trattamento dei Dati con il supporto della Struttura AILCAT, sotto il controllo del DPO/RPD.

7.5 FASE 5: ANALISI POST VIOLAZIONE

L'ultima fase del processo di gestione delle Violazioni di Dati Personali prevede 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.
Tale attività prevede il coinvolgimento, laddove necessario, delle funzioni dei Sistemi informativi, con eventuale supporto da parte di altre aree funzionali.

7.6 "DATA BREACH" PRESSO L' ASL O UN TERZO IN QUALITÀ DI RESPONSABILE ESTERNO

OBBLIGHI DI COMUNICAZIONE DELL'ENTE QUANDO OPERA IN QUALITÀ DI RESPONSABILE

Quando l'Ente agisce in qualità di Responsabile, in caso di Violazione dei Dati Personali, deve informare il Titolare, senza ingiustificato ritardo, secondo i tempi ed i modi concordati nel contratto per il Trattamento dei Dati Personali trasmesso da quest'ultimo.

OBBLIGHI DI COMUNICAZIONE DI UN RESPONSABILE NEI CONFRONTI DELL'ENTE

Nel caso in cui vi sia la presenza di un terzo che agisca in qualità di Responsabile del Trattamento, al verificarsi di una Violazione dei Dati Personali, questi deve informare l'ASL (in qualità di Titolare), senza ingiustificato ritardo e, non oltre le 24 ore dal momento in cui ha conoscenza della Violazione, inviando una comunicazione ai seguenti indirizzi: e-mail rpd@asl.novara.it, PEC protocollogenerale@pec.asl.novara.it e, successivamente, collaborare con l'Ente per consentire alla stessa di adempiere agli obblighi previsti dalla normativa agli artt. 33 e 34 del GDPR.
Il Responsabile deve assistere l'Ente avviando un'analisi preliminare finalizzata alla raccolta dei Dati concernenti l'anomalia ed alla compilazione della Scheda Evento utilizzando il modello allegato alla presente Procedura.

Una volta condotta l'analisi preliminare, il Responsabile deve procedere all'analisi di primo livello per verificare che la segnalazione non tratti un "falso positivo". All'esito dell'accertamento, qualora si tratti di un "falso positivo", il Responsabile deve comunicarlo immediatamente all'Ente agli stessi indirizzi sopra indicati, al fine di consentire l'inserimento del evento nella sezione "eventi falsi positivi" del Registro dei "Data Breach" (Cfr. Cod. 024/Mod/19/Rev.n).
In caso contrario, il Responsabile recupera le informazioni di dettaglio sull'evento, necessarie alle analisi di secondo livello, e le riporta nella Scheda Evento che deve essere inviata, possibilmente via PEC, tempestivamente e, non oltre 24 ore dalla conoscenza della Violazione, al Titolare e al DPO, i quale devono essere costantemente tenuti aggiornati.
L'evento deve essere inserito nell' apposito Registro dei "Data Breach".
L'ASL, una volta ricevuta la Scheda Evento, deve procedere secondo le fasi del processo descritto nelle sezioni precedenti.

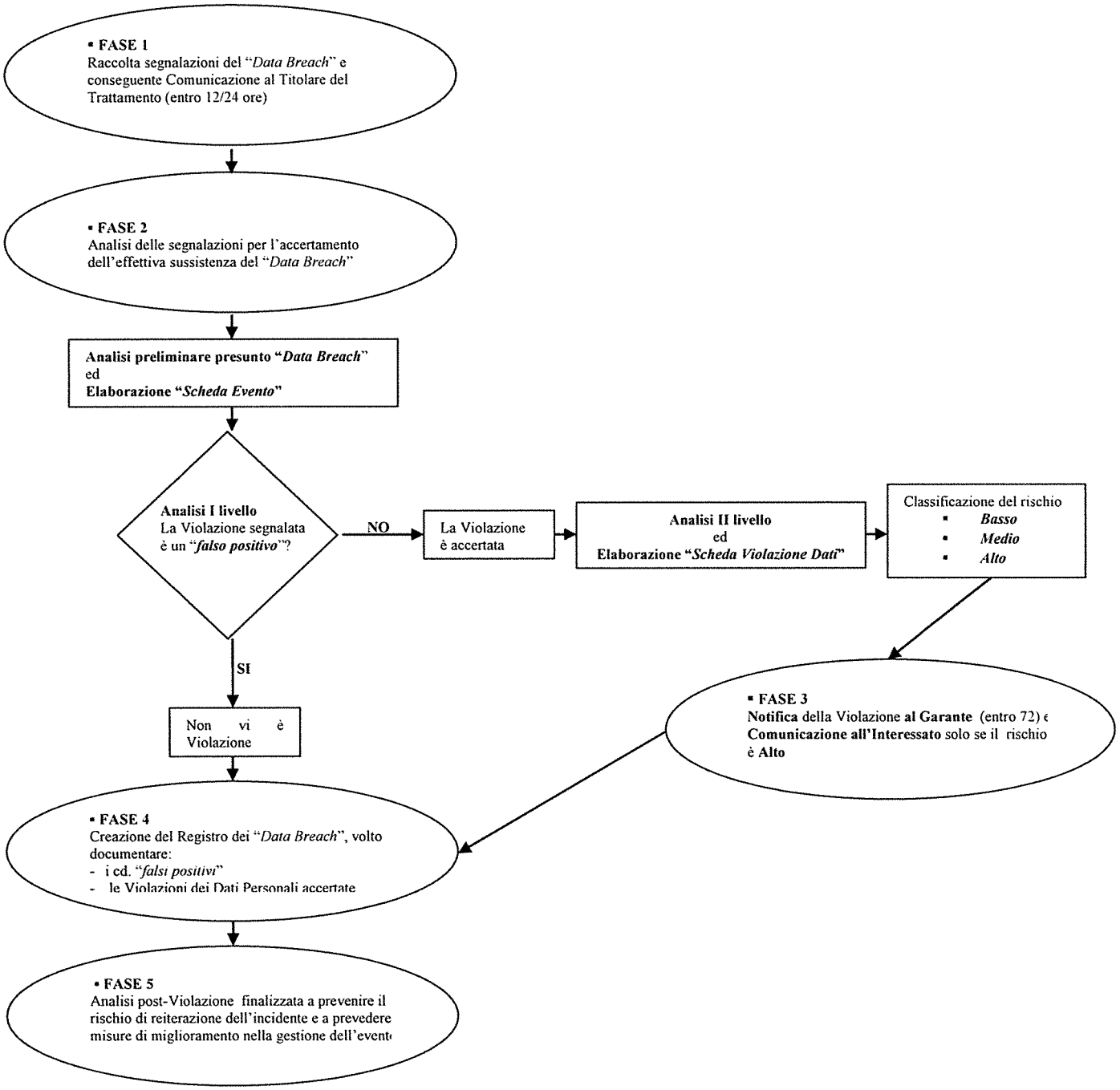
La tabella successiva sintetizza il processo descritto:

AZIONE	RESPONSABILITÀ	MODALITÀ	TEMPISTICA
Presa in carico delle segnalazioni	USP	Raccolta della segnalazione pervenuta dai canali interni ed esterni	Non appena pervenuta la segnalazione
Analisi di I livello	USP	Raccolta e recupero delle informazioni necessarie all'analisi di II livello e all'individuazione dei falsi positivi con eventuale coinvolgimento delle Strutture aziendali interessare dall'evento	Entro 12/24 ore dalla conoscenza dell'evento
Raffinamento regole per individuazione falsi positivi	SICG	Analisi cause che hanno indotto a segnalazione di falso positivo. Individuazione migliorie e comunicazione via email esito analisi a USP.	Entro 7 gg dall'evento

AZIONE	RESPONSABILITÀ	MODALITÀ	TEMPISTICA
Analisi II livello e redazione della Scheda Violazione Dati	USP	Analisi di tutti gli eventi ed individuazione degli elementi per redazione scheda violazione dati. Decisione su azioni da intraprendere e misure da adottare per minimizzare le conseguenze negative della Violazione.	Nei termini utili per effettuare la notifica all'Autorità di Controllo entro le 72 ore
Notifica all'autorità di Controllo	DG con supporto AILCAT	Invio PEC del modulo previsto dal Garante per la protezione dei dati personali e reperibile sul sito	Entro 72 ore
Comunicazione della violazione all'interessato	DG con supporto AILCAT	La comunicazione deve essere effettuata quando si rilevi un rischio per i diritti e le libertà delle persone fisiche classificato come ALTO nella Scheda Violazione Dati	Non appena ultimata la valutazione della violazione
Registrazione scheda evento nel registro dei "Data breach"	AILCAT	Compilazione delle informazioni sull'evento nel registro anche in caso anche di falso positivo	Entro 72 ore
Analisi post incidente	USP	Analisi delle informazioni raccolte nel contesto dell'evento per valutare l'efficacia ed efficienza delle azioni intraprese nella gestione dell'evento	Entro 30 gg dalla chiusura dell'evento
Comunicazione dell'ASL al Titolare nel caso in cui l'ASL sia Responsabile esterno del Trattamento	DG con supporto USP	Secondo le modalità concordate nell'atto di nomina	Secondo le tempistiche concordate nell'atto di nomina

7.7 DIAGRAMMA PROCESSO DI GESTIONE "DATA BREACH"

Il diagramma che segue riporta, in maniera sintetica, le fasi del Processo di gestione dei "Data Breach", sopra descritto:



8. INDICATORI

Criterio	Indicatore	Standard atteso	Modalità e Tempistica di rilevazione
% eventi notificati nei termini	N. eventi notificati entro 72 ore/numero di eventi totali soggetti a notifica	90%	AILCAT Rilevazione annuale
% falsi positivi	N. eventi falsi positivi/numero totale di segnalazioni	<30%	AILCAT Rilevazione annuale

9. LISTA DI DISTRIBUZIONE

VD – AILCAT - DMPO – SICG – COLLEGIO SINDACALE.

10. BIBLIOGRAFIA

- Regolamento UE 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016;
- D. Lgs. 30 giugno 2003, n° 196, nel testo novellato dal d. Lgs. 10 agosto 2018, n° 101;
- Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali (doc. web n. 9126951).

11. ALLEGATI

Tipologia	Codice allegato	Descrizione
Modulistica	*026/Mod/19/Rev.n*	Scheda evento
Modulistica	*025/Mod/19/Rev.n*	Scheda violazione dati
Modulistica	*024/Mod/19/Rev.n*	Registro dei Data Breach
Modulistica	*027/Mod/19/Rev.n*	Modello di comunicazione all'interessato della violazione dei dati personali

364 2 OTT. 2019

	REGISTRO DEI DATA BREACH	COD: 024/Mod/19/Rev.0

Il seguente format di registro potrà essere realizzato anche in formato elettronico, richiamando i seguenti campi

Evento				**Conseguenze**	**Provvedimenti adottati**	**Notifica all'autorità di controllo**		**Comunicazione all'interessato**	
Codice 4	Irrilevante	Falso Positivo	Rilevante			SI/NO	Data	SI/NO	Data

REGISTRO DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)							
n.	**DATA VIOLAZIONE**	**N° SCHEDA EVENTO**	**N. INTERESSATI COINVOLTI**	**NOTIFICA AL GARANTE (X)**		**COMUNICAZIONE AGLI INTERESSATI**	
1				SI	NO	SI	NO
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)
2				SI	NO	SI	NO
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)
3				SI	NO	SI	NO
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)
4				SI	NO	SI	NO
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)
5				SI	NO	SI	NO
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)

364 - 2 OTT. 2019

	SCHEDA VIOLAZIONE DATI	COD: 025/Mod/19/Rev.0

CODICE EVENTO 1	CLASSIFICAZIONE 2	RISCHIO 3

Il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche anche diverse dall'interessato a cui si riferiscono i dati, a causa della violazione dei dati personali:

- discriminazioni
- furto o usurpazione d'identità
- perdite finanziarie
- pregiudizio alla reputazione
- perdita di riservatezza dei dati personali protetti da segreto professionale
- decifratura non autorizzata della pseudonimizzazione
- danno economico o sociale significativo
- privazione o limitazione di diritti o libertà
- impedito controllo sui dati personali all'interessato
- danni fisici, materiali o immateriali alle persone fisiche.
- impedito controllo sui dati personali all'interessato
- danni fisici, materiali o immateriali alle persone fisiche.

N.B. Griglia di classificazione

Classificazione di rischio	**Codice**	**Gravità della Violazione**	**Codice**	**Classificazione evento**
BASSO/TRASCURABILE	RISCHIO 1	BASSO/TRASCURABILE	1	Irrilevante
MEDIO	RISCHIO 2	MEDIO	2	Falso Positivo
ALTO	RISCHIO 3	ALTO	3	Rilevante
MOLTO ALTO	RISCHIO 4	MOLTO ALTO	4	Grave (Cod. 4)

364 - 2 OTT. 2019

	SCHEDA EVENTO	COD: 026/Mod/19/Rev.0

SCHEDA EVENTO					
EVENTO				**PROVVEDIMENTI**	
DATA EVENTO		**DATA E ORA DI CONOSCENZA**		**NOTIFICA AL GARANTE (X)**	
ORA EVENTO		**SEGNALANTE**		SI	NO
LUOGO DELLA VIOLAZIONE		**NATURA EVENTO**		(inserire data di notifica)	(motivare mancata notifica)
ENTE/SOCIETA' COINVOLTO/A		**N. INTERESSATI COINVOLTI**			
CATEGORIE DI DATI INTERESSATI		**CATEGORIE DI INTERESSATI COINVOLTI**		**(eventuale) COMUNICAZIONE ALL'INTERESSATO**	
				SI	NO
				(inserire data di comunicazione	(motivare mancata comunicazione)
				INTERVENTI DI RIPRISTINO (RECOVERY)	
CONSEGUENZE VIOLAZIONE		**SISTEMI E DISPOSITIVI COINVOLTI**			
				TEMPO DI RIPRISTINO (RECOVERY)	
DESCRIZIONE ANALITICA DELL'EVENTO				**ULTERIORI AZIONI DA INTRAPRENDERE**	
CODICE EVENTO					
DATA DI COMPILAZIONE		FIRMA			
LUOGO DI COMPILAZIONE					
DATA ULTIMA MODIFICA					

364 - 2 OTT. 2019

	MODELLO DI COMUNICAZIONE ALL'INTERESSATO DELLA VIOLAZIONE DEI DATI PERSONALI	CODICE: 027/Mod/19/Rev.0

MODELLO DI COMUNICAZIONE ALL'INTERESSATO DELLA VIOLAZIONE DEI DATI PERSONALI

Nota: Il seguente modello illustra le modalità di comunicazione di una Violazione. Rispetto ai diversi campi indicati dovrà essere scelta l'opzione che si può riferire allo specifico caso, in base agli esempi riportati.

Secondo quanto prescritto dall'art. 34 del Regolamento Generale in materia di protezione dei dati personali RE (UE) n. 679/2016, l'ASL NOVARA, Titolare del Trattamento, con la presente è a comunicarLe, l'intervenuta Violazione dei Suoi Dati Personali (Data breach)

- *che si è verificata:*

A. in data _____, alle ore_____;
B. tra il _____ed il_____;
C. in un tempo non ancora determinato;
D. è possibile che sia ancora in corso.

- *di cui si è avuto conoscenza in data _____alle ore_____.*

A) Descrizione della natura della Violazione:

_____
_____
_____
_____
_____
_____
_____
_____

1) Dove è avvenuta la Violazione dei Dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili).

_____
_____
_____
_____

2) Tipo di Violazione, per esempio:
- ☐ 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 _____

REGIONE PIEMONTE A.S.L. NO AZIENDA REGIONALE

3) Dispositivo oggetto di Violazione, per esempio:
- ☐ computer
- ☐ rete
- ☐ dispositivo mobile
- ☐ strumento di backup
- ☐ documento cartaceo
- ☐ altro _____

4) Descrizione dei sistemi di elaborazione o di memorizzazione dei Dati coinvolti, con indicazione della loro ubicazione:

_____
_____
_____
_____
_____
_____
_____
_____

5) Che tipo di Dati sono oggetto di Violazione, per esempio:
- ☐ Dati anagrafici (nome, cognome, numero di telefono, e mail, CF, indirizzo ecc..)
- ☐ Dati di accesso e di identificazione (username, password, customer ID, altro)
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica
- ☐ Dati personali idonei a rivelare le convinzioni religiose
- ☐ Dati personali idonei a rivelare filosofiche o di altro genere
- ☐ Dati personali idonei a rivelare le opinioni politiche
- ☐ Dati personali idonei a rivelare l'adesione a partiti
- ☐ Dati personali idonei a rivelare sindacati,
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere religioso
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere filosofico
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere politico
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere sindacale
- ☐ Dati personali idonei a rivelare lo stato di salute
- ☐ Dati personali idonei a rivelare la vita sessuale
- ☐ Dati giudiziari
- ☐ Dati genetici
- ☐ Dati biometrici
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ Altro _____

B) Descrivere le probabili conseguenze della Violazione dei Dati Personali;

_____
_____
_____
_____

C) Descrivere quali sono le misure tecnologiche ed organizzative assunte per porre rimedio alla Violazione e, se del caso, per contenere la Violazione dei Dati o per attenuarne i possibili effetti negativi;

_____

_____

_____

_____

Per poter ottenere maggiori informazioni relativamente alla Violazione in oggetto, può contattare l'ufficio scrivente _____ *[[DPO/funzione legale /funzione competente da identificarsi] ai seguenti indirizzi*:

Dati di contatto:
a) nome e cognome del DPO/RPD (*ove esistente*): _____
b) indirizzo di posta elettronica: _____
c) indirizzo di posta PEC: _____
d) indirizzo posta cartacea: _____
e) numero telefonico dedicato: _____
f) numero di fax dedicato: _____

Data, Luogo _____

Il Titolare del Trattamento

_____

[il DPO]

_____

Distinti saluti

PROVVEDIMENTO NUMERO 364 **DEL** - 2 OTT. 2019

AFFARI ISTITUZIONALI, LEGALI, COMUNICAZIONE, ANTICORRUZIONE E TRASPARENZA

FOGLIO ADEMPIMENTI
- EFFETTI -

- ***Il presente provvedimento è esecutivo***:

  [X] ***Giorno inizio esecutività*** _____

  [ ] ***dal giorno della sua iscrizione nel Registro Generale***

  [ ] ***dalla data in esso provvedimento indicata***

- PUBBLICAZIONE -

Al presente provvedimento è stata data pubblicità legale, ai sensi dell'art. 32, 1° comma, L. 69/2009, tramite pubblicazione sul sito informatico dell'Ente ad iniziare dal giorno 18 OTT. 2019

REGIONE PIEMONTE A.S.L. NO AZIENDA REGIONALE

AFFARI ISTITUZIONALI, LEGALI, COMUNICAZIONE, ANTICORRUZIONE E TRASPARENZA
IL DIRETTORE
(dott. Claudio Terrugi)

* * * * * *

- COMUNICAZIONI -

Provvedimento trasmesso in copia alle sottospecificate Strutture aziendali

[X] **V.D.** [X] **COLLEGIO SINDACALE**

[X] **AILCAT**	[ ] **SEF**	[ ] **GPVRU**	[ ] **STP**
[X] **SICG**	[X] **DMPO**	[ ] **DIPSA**	[ ] **DEA**
[ ] **GOCSS**	[ ] **SPS**	[ ] **FO**	[ ] **FT**
[ ] **SPP**	[ ] **MC**	[ ] **SEPI**	[ ] **ACEP**
[ ] **ASSTERR**	[ ] **PALLIATIVE**	[ ] **SANPEN**	[ ] **COTESS**
[ ] **SML**	[ ] **DSM**	[ ] **DMI**	[ ] **DPD**
[ ] **API**	[ ] **CCP**	[ ] **DAN**	[ ] **DAS**
[ ] **DUN**	[ ] **DP**	[ ] **SISP**	[ ] **SIAN**
[ ] **SIAV**	[ ] **SPRESAL**	[ ] **UVOS**	[ ] **DADES**

[ ] **ALTRI** _____

_____

REGIONE PIEMONTE A.S.L. NO AZIENDA REGIONALE