REGIONE TOSCANA
AZIENDA UNITA' SANITARIA LOCALE TOSCANA CENTRO
Sede Legale Piazza Santa Maria Nuova n. 1 – 50122 Firenze

DELIBERA DEL DIRETTORE GENERALE

Numero della delibera	250
Data della delibera	28-02-2020
Oggetto	Procedure aziendali
Contenuto	Sistema Aziendale Privacy: adozione procedura violazione dei dati

Dipartimento	DIREZIONE AMMINISTRATIVA AZIENDALE
Direttore Dipartimento	PESCINI LORENZO
Struttura	SOC AFFARI GENERALI
Direttore della Struttura	CARLINI LUCIA
Responsabile del procedimento	CAGNONI SARA

Conti Economici			
Spesa	**Descrizione Conto**	**Codice Conto**	**Anno Bilancio**
Spesa prevista	**Conto Economico**	**Codice Conto**	**Anno Bilancio**

Estremi relativi ai principali documenti contenuti nel fascicolo		
Allegato	**N° pag.**	**Oggetto**
A	8	procedura Aziendale violazione dei dati
1	2	esempi di violazioni dei dati
2	1	diagramma di flusso gestione violazione dati
3	1	diagramma di flusso notifica

"documento firmato digitalmente"

IL DIRETTORE GENERALE
(in forza del D.P.G.R. Toscana n. 33 del 28 febbraio 2019)

Vista la Legge Regionale n. 84/2015 recante "*Riordino dell'assetto istituzionale e organizzativo del Sistema Sanitario Regionale. Modifiche alla Legge Regionale 40/2005*";

Vista la delibera n. 1720 del 24.11.2016 di approvazione dello Statuto aziendale e le conseguenti delibere di conferimento degli incarichi dirigenziali delle strutture aziendali;

Premesso che:
- il Parlamento Europeo ed il Consiglio in data 27/04/2016 hanno approvato il Regolamento Europeo 2016/679 (RGPD) concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, che ha abrogato la direttiva 95/46/CE;
- il suddetto Regolamento è entrato in vigore il 24 Maggio 2016 ed è divenuto definitivamente applicabile in via diretta in tutti gli Stati Membri a partire dal 25 Maggio 2018;
- il D.Lgs 101/2018 (cd. decreto di adeguamento) recante *"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)" che è intervenuto modificando il D.Lgs 196/03 ed abrogando, fra l'altro, il Titolo IV relativo ai "soggetti che effettuano il trattamento";*
- il Gruppo di Lavoro articolo 29 sulla protezione dei dati ha adottato in data 3/10/2017 e smi le Linee Guida sulla notifica delle violazioni dei dati ai sensi del regolamento UE 2016/679;
- l'Azienda USL Toscana Centro, è Titolare del trattamento dei dati personali effettuato durante lo svolgimento della propria attività istituzionale come da prima notificazione n. 2016031700221268 (numero iscrizione registro notificazioni);

Richiamati i seguenti atti:
- la deliberazione n. 179 del 30/01/2019 con la quale sono state assunte precise determinazioni inerenti all'assetto organizzativo per la gestione del sistema aziendale privacy al fine di rispettare gli obblighi organizzativi, documentali e tecnici, con l'obiettivo di attuare la piena e consapevole applicazione del nuovo quadro normativo in materia di trattamento dei dati personali perfezionatosi con l'entrata in vigore in data 19/09/2018 del D.Lgs 101/2018 cd. decreto di adeguamento;
- la determina n. 2711 del 24/12/2019 con la quale è stato affidato il servizio di Responsabile della Protezione dei dati personali (RPD) ai sensi del Regolamento UE 2016/679 all'Avv. Michele Morriello;

Considerato che:
- Il regolamento generale sulla protezione dei dati ha disposto la notifica obbligatoria in caso di violazioni dei dati personali, per tutti i titolari del trattamento a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. I responsabili del trattamento hanno un ruolo importante da svolgere e devono notificare qualsiasi violazione al proprio titolare del trattamento.

Rilevato che:
- con nota email del 19/03/2019 è stata data specifica comunicazione a tutti i Referenti del trattamento dei dati in materia di violazioni dei dati personali precisando in particolare gli adempimenti previsti dalla normativa;
- sono stati effettuati 12 edizioni del corso di formazione privacy rivolto ai Referenti del trattamento dei dati ove è stata analizzata, fra l'altro, cosa significa violazione dei dati personali e come procedere in caso di violazione;

Ritenuto, necessario, ratificare con specifica procedura il percorso da attivare in caso di violazioni dei dati in conformità a quanto stabilito dagli artt.33 e 34 del regolamento UE 2016/679;

Dato atto che:
- la predisposizione della procedura in oggetto è stata condivisa con i componenti del Gruppo di lavoro protezione dei dati coordinato dal Responsabile della Protezione dei Dati, in diversi incontri del gruppo e precisamente nelle date 8/11/2019 e 6/12/ 2019;
- con email del 19/12/2019 è stata inviata al gruppo di lavoro la proposta di procedura come condivisa in sede di incontro, al fine di raccogliere ulteriori osservazioni in merito;

Preso atto che il Direttore della SOC Affari Generali – Dr.ssa Lucia Carlini nel proporre il presente atto attesta la regolarità tecnica ed amministrativa e la legittimità e congruenza dell'atto con le finalità istituzionali di questo Ente, stante anche l'istruttoria, condivisa con il Responsabile della protezione dei dati Avv.Michele Morriello ed effettuata, a cura del Responsabile del Procedimento, Dr.ssa Sara Cagnoni , in servizio c/o la SOC Affari generali.;

Su proposta del Direttore della SOC Affari Generali – Dr.ssa Lucia Carlini;

Acquisito il parere favorevole del Direttore Amministrativo, del Direttore Sanitario e del Direttore dei Servizi Sociali;

DELIBERA

per i motivi espressi in narrativa:

1. **di adottare** la procedura aziendale violazione dei dati personali unita al presente atto quale parte integrante e sostanziale sotto la voce di allegato A) comprensiva dei sub-allegati 1) 2) e 3);

2. **di revocare** ogni e qualsiasi altro atto in contrasto con la presente deliberazione;

3. **di incaricare** il Responsabile del Procedimento di dare informazione del presente atto a tutti i Referenti ed Incaricati del trattamento dei dati anche tramite il Portale della privacy sezione Cruscotto – inserito sul sito intranet, previa comunicazione email a tutti i referenti del trattamento dei dati ;

4. **di stabilire** che le strutture aziendali che stipulano convenzioni o contratti con soggetti esterni all'Azienda devono dare comunicazione della presente deliberazione ai soggetti esterni individuati quali Responsabili del trattamento dei dati ai sensi dell'art.28 del Regolamento UE 2016/679;

5. **di incaricare** i Referenti del trattamento dei dati ad adempiere alle disposizioni emanate in materia, verificando l'applicazione delle stesse da parte del personale assegnato, individuato "incaricato al trattamento dei dati" e fornendogli le istruzioni per l'adozione di comportamenti corretti in materia di tutela della riservatezza e protezione del dato;

6. **di stabilire** che i Referenti e gli Incaricati del trattamento dei dati si impegnano, fra l'altro, a prestare la massima collaborazione nei confronti del Titolare e del Responsabile della Protezione dei Dati fornendo tutte le informazioni richieste al fine di dare compimento agli adempimenti previsti dalla normativa vigente in materia di protezione dei dati personali;

7. **di trasmettere**, a cura del Responsabile del procedimento, la presente delibera al Dipartimento Risorse Umane;

8. **di incaricare** la S.O.C Politiche e Relazioni Sindacali, di trasmettere copia del presente atto alle OOSS delle tre Aree negoziali ed alla RSU aziendale ai sensi delle disposizioni vigenti in materia;

9. **di dichiarare** la presente deliberazione immediatamente eseguibile al fine di dare immediato avvio alla procedura in conformità con l'intervenuto quadro normativo di riferimento;

10. **di trasmettere** la presente deliberazione al Collegio Sindacale a norma di quanto previsto dall' art. 42 comma 2, della L.R.T. 40/2005 e ss.mm.ii.

IL DIRETTORE GENERALE
(Dr. Paolo Morello Marchese)

IL DIRETTORE AMMINISTRATIVO
(Dr. Lorenzo Pescini)

IL DIRETTORE SANITARIO
(Dr. Emanuele Gori)

IL DIRETTORE DEI SERVIZI SOCIALI
(Dr.ssa Rossella Boldrini)

PROCEDURA VIOLAZIONE DEI DATI

Data	Redazione	Verifica	Approvazione
29/01/2020	P.O. privacy e supporto Data protection officer – Sara Cagnoni -	**Processo** Responsabile protezione dati - Michele Morriello **SGQ** SOC Affari Generali – Lucia Carlini	Direttore Amministrativo Lorenzo Pescini

Gruppo di redazione – componenti Gruppo di lavoro protezione dati:

- Emanuele Croppi (Direttore Dipartimento Medicina Generale)
- Ilaria Perigli – Barbara Lazzari (Staff Direttore Generale)
- Daniela Matarrese (Direttore Dipartimento Rete Ospedaliera)
- Alessandro Sergi – Pierluigi Perruccio (Staff Direzione Sanitaria)
- Lucia Carlini (Direzione Amministrativa)
- Alessandro Natali (Dipartimento delle Specialistiche Mediche)
- Giovanni Benelli (Dipartimento delle Specialistiche Chirurgiche)
- Daniela Matteuzzi (Dipartimento Emergenza e Area critica)
- Marco Pezzati (Direttore Dipartimento Materno Infantile)
- Carlo Milandri (Dipartimento Oncologico)
- Martina Boni (Dipartimento di Medicina Fisica e Riabilitazione)
- Grazia Gentilini (Dipartimento di medicina di laboratorio)
- Adriano Viviani (Dipartimento Diagnostica per Immagini)
- Daniele Romeo – Benedetta Novelli (Dipartimento Rete Sanitaria Territoriale)
- Donella Posarelli (Dipartimento Salute mentale e Dipendenze)
- Alberto Anichini (Dipartimento del Farmaco)
- Rosaria Raffaelli – Marco Alaimo (Dipartimento Assistenza Infermieristica ed Ostetrica)
- Riccardo Valencetti (Dipartimento Servizi Tecnico Sanitari)
- Nadia Betti (Dipartimento della prevenzione)
- Mery Cai – Azzurra Staderi (Dipartimento Servizi Sociali)
- Sonny Paccagnini – Sergio Biagini (Dipartimento Risorse Umane)
- Rita Bonciani (Direttore Dipartimento Decentramento)
- Marco Brintazzoli (Direttore Dipartimento Area tecnica)
- Claudia Galanti – Gabriele Bini (Dipartimento Amministrazione, Pianificazione e Controllo di Gestione)
- Sergio Lami (Direttore Dipartimento Interaziendale SIOR)

Parole chiave: procedura, dati, violazione

INDICE GENERALE

PREMESSA 2
ART.1 SCOPO E AMBITO DI APPLICAZIONE 2
ART.2 POLITICHE DI SICUREZZA 3
ART.3 TIPI DI VIOLAZIONI DEI DATI PERSONALI 3
ART.4 PROCEDURA DI GESTIONE DI UNA VIOLAZIONE DEI DATI (allegati 1e 2 esempi di violazione dei dati e diagramma di flusso gestione violazione dati) 3
ART. 5 VALUTAZIONE DELL'ESISTENZA DI UN RISCHIO O DI UN RISCHIO ELEVATO 5
ART. 6 NOTIFICA ALL'AUTORITÀ DI CONTROLLO (allegato 3 diagramma di flusso notifica) 5
ART.7 INFORMARE L'INTERESSATO 6
ART. 8 RESPONSABILIZZAZIONE E TENUTA DI REGISTRI 7
ART. 9 SANZIONI E RESPONSABILITA' 7
ART.10 RIFERIMENTI NORMATIVI 7
ART. 11 ALLEGATI 8
ART. 12 INDICE DI REVISIONE 8
ART. 13 LISTA DI DIFFUSIONE 8

PREMESSA

Il regolamento generale sulla protezione dei dati, Regolamento Europeo 679/2016 (di seguito Regolamento) introduce l'obbligo di notificare una violazione dei dati personali (di seguito "violazione") all'autorità di controllo nazionale competente (oppure, in caso di violazione transfrontaliera, all'autorità capofila) e, in alcuni casi, di comunicare la violazione alle singole persone fisiche i cui dati personali sono stati interessati dalla violazione. La notifica è obbligatoria per tutti i titolari del trattamento a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Anche i responsabili del trattamento hanno un ruolo importante da svolgere e devono notificare qualsiasi violazione al proprio titolare del trattamento.

ART.1 SCOPO E AMBITO DI APPLICAZIONE

1. La presente procedura individua gli obblighi di notifica e di comunicazione delle violazioni sanciti dal Regolamento e si applica soltanto in caso di violazione di dati personali.

ART.2 POLITICHE DI SICUREZZA

1. Il Titolare[1] ed il Responsabile[2] del trattamento dei dati si impegnano a predisporre le misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati, tenendo conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento nonchè del rischio e gravità per i diritti e le libertà delle persone fisiche.
2. Il Titolare ed il Responsabile del trattamento dei dati si impegnano a mettere in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata una violazione dei dati personali al fine di determinare l'obbligatorietà dell'obbligo di notifica. Di conseguenza, un aspetto fondamentale di qualsiasi politica di sicurezza dei dati è la capacità, ove possibile, di prevenire una violazione e, laddove essa si verifichi ciò nonostante, di reagire tempestivamente.

ART.3 TIPI DI VIOLAZIONI DEI DATI PERSONALI

1. La violazione dei dati personali è una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Le violazioni possono essere classificate in base ai tre principi della sicurezza delle informazioni (c.d. parametro RID):
   a. violazione della riservatezza, in caso di divulgazione, anche accidentale, dei dati personali o accesso agli stessi ad opera di soggetti non autorizzati;
   b. violazione dell'integrità, in caso di modifica e/o alterazione non autorizzata o accidentale dei dati personali;
   c. violazione della disponibilità, in caso di perdita o distruzione accidentali o non autorizzati di dati personali.
2. Il titolare del trattamento dovrà valutare la probabilità e la gravità dell'impatto dell'evento relativo ai dati personali sui diritti e sulle libertà delle persone fisiche sia nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione) sia nel caso di una violazione che implichi la perdita temporanea di disponibilità.
3. Una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

ART.4 PROCEDURA DI GESTIONE DI UNA VIOLAZIONE DEI DATI (allegati 1e 2 esempi di violazione dei dati e diagramma di flusso gestione violazione dati)

1. **Il Referente** del trattamento dei dati che sia venuto a conoscenza, direttamente o indirettamente, di una violazione dei dati ne informa il Titolare e il Responsabile

[1] Definizione: il titolare del trattamento è 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 (Azienda USL Toscana centro).
[2] Definizione: il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (soggetto esterno all'Azienda USL TC).

della protezione dei dati (di seguito RPD) senza ingiustificato ritardo e, comunque entro 24 ore da quando ne è venuto a conoscenza. L'invio dovrà essere formalizzato attraverso la comunicazione tramite posta elettronica ai soggetti indicati, richiedendo conferma di lettura e sincerandosi, comunque, che l'invio della comunicazione sia andato a buon fine.

2. I**l Responsabile** del trattamento dei dati (individuato ex art.28) si impegna a notificare al Titolare ogni violazione dei dati personali, senza ingiustificato ritardo dall'avvenuta conoscenza, e comunque entro 72 ore, con comunicazione da inviarsi all'indirizzo PEC del titolare.
3. Il Responsabile ed il Referente del trattamento dei dati provvedono alla segnalazione di cui ai commi 1 e 2 avendo cura di fornire almeno le informazioni previste al successivo art.6, comma 1, lettere a), c) e d), omettendo di includere nella comunicazione via email i dati personali degli interessati coinvolti nella violazione.
4. Il Referente ed il Responsabile, qualora non procedano a comunicare la violazione dei dati di cui siano venuti a conoscenza al Titolare, con le modalità e la tempistica di cui ai precedenti punti, si assumono ogni responsabilità in ordine alla sanzione o al danno che al Titolare possano derivare da tale omissione o ritardo.
5. Il RPD, tempestivamente e senza ingiustificato ritardo, nel momento in cui è venuto a conoscenza di una violazione dei dati e al fine di consentire al Titolare la valutazione preliminare sulle probabilità e gravità dei rischi per i diritti e le libertà degli interessati che possono derivare, provvede con le modalità più idonee a coinvolgere:
   - il Referente/i del trattamento dei dati oggetto di violazione;
   - Il Responsabile/i del trattamento dei dati oggetto di violazione;

   Provvede, inoltre, a coinvolgere, se necessario:
   - il soggetto designato a livello dipartimentale quale componente del gruppo di lavoro protezione dati interessato dalla violazione dei dati;
   - il soggetto designato dallo Staff Direzione Aziendale SOC Organizzazione e Progetti Tecnologici, componente del gruppo lavoro protezione dati;
   - il Referente tecnico-informatico designato da ESTAR, a supporto dell'Azienda su problematiche di sicurezza;
   - ogni altro soggetto che ritenga utile coinvolgere ai fini istruttori.
6. Il RPD curerà e documenterà l'attività istruttoria, acquisendo tutti gli elementi necessari per l'effettuazione della valutazione. All'esito di tale attività che deve compiersi tempestivamente e, comunque, in modo da poter notificare la violazione entro il termine di 72 ore dall'avvenuta conoscenza della violazione, il RPD redige un verbale corredato dalla documentazione di supporto e da una proposta operativa da sottoporre al Titolare.
7. Il RPD redige gli eventuali atti di notifica al Garante e l'eventuale comunicazione all'interessato o agli interessati e li sottopone al Titolare del Trattamento per la sottoscrizione.
8. I soggetti aziendali interessati dalla violazione dei dati devono fornire la massima collaborazione al RPD; eventuali comportamenti non collaborativi, ostruzionistici e/o omissivi e/o reticenti saranno segnalati alla Direzione Aziendale al fine di una

valutazione anche ai fini disciplinari.

9. Il Responsabile si impegna a prestare ogni più ampia assistenza al Titolare al fine di consentirgli di assolvere agli obblighi di cui agli artt. 33 - 34 del GDPR. Una volta definite le ragioni della violazione, il Responsabile di concerto con il Titolare e/o altro soggetto da quest'ultimo indicato, su richiesta, si attiverà per implementare nel minor tempo possibile tutte le misure di sicurezza fisiche e/o logiche e/o organizzative atte ad arginare il verificarsi di una nuova violazione della stessa specie di quella verificatasi, al riguardo anche avvalendosi dell'operato di subfornitori.
10. I soggetti sopra individuati – Titolare – RPD - Responsabile – Referente si considerano "a conoscenza" di una violazione nel momento in cui sono ragionevolmente certi che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali. I soggetti citati possono effettuare una breve indagine per stabilire se la violazione si sia effettivamente verificata. Durante il periodo di indagine il titolare, responsabile, referente del trattamento non possono essere considerati "a conoscenza". Tuttavia, si prevede che l'indagine iniziale inizi il più presto possibile e stabilisca con ragionevole certezza se si è verificata una violazione; può quindi seguire un'indagine più dettagliata.

ART. 5 VALUTAZIONE DELL'ESISTENZA DI UN RISCHIO O DI UN RISCHIO ELEVATO

1. Il rischio come fattore che determina l'obbligo di notifica:
   a. la notifica all'autorità di controllo competente è obbligatoria a meno che sia improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche. Sono quindi oggetto di notifica unicamente le violazioni di dati personali che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali;
   b. la comunicazione di una violazione alle persone fisiche diventa necessaria soltanto laddove la violazione possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche
2. Fattori da considerare nella valutazione del rischio:
   a. Il tipo di violazione verificatosi può influire sul livello di rischio presentato per le persone fisiche;
   b. Natura, carattere sensibile e volume dei dati personali;
   c. Facilità di identificazione delle persone fisiche;
   d. Gravità delle conseguenze per le persone fisiche;
   e. Caratteristiche particolari dell'interessato;
   f. Caratteristiche particolari del titolare del trattamento di dati;
   g. Numero di persone fisiche interessate.

ART. 6 NOTIFICA ALL'AUTORITÀ DI CONTROLLO (allegato 3 diagramma di flusso notifica)

1. Il Titolare del trattamento notifica la violazione dei dati all'autorità di controllo, entro 72 ore dal momento in cui è venuto a conoscenza, la notifica non deve includere i dati personali oggetto di violazione e deve contenere le informazioni previste all'articolo 33, paragrafo 3, del Regolamento e indicate nel modello

allegato al provvedimento del garante del 30/07/2019 come di seguito elencato:
a.descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b.comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c.descrivere le probabili conseguenze della violazione dei dati personali;
d.descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi".

2. A seconda della natura della violazione, il titolare del trattamento può avere la necessità di effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente, pertanto, qualora non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
3. La notifica all'autorità di controllo, qualora non sia effettuata entro 72 ore, deve essere corredata dei motivi del ritardo. Questa disposizione, unitamente al concetto di notifica in fasi, riconosce che il titolare del trattamento potrebbe non essere sempre in grado di notificare una violazione entro tale termine e che una notifica tardiva può essere consentita.

ART.7 INFORMARE L'INTERESSATO

1. il Titolare del trattamento, oltre a effettuare la notifica all'autorità di controllo, è tenuto a comunicare la violazione alle persone fisiche interessate se questa comporta un rischio elevato per i diritti e le libertà delle persone, senza ingiustificato ritardo.
2. Ai fini della comunicazione alle persone fisiche, secondo l'articolo 34, paragrafo 2, il titolare del trattamento deve fornire almeno le seguenti informazioni:
   a. una descrizione della natura della violazione;
   b. il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
   c. una descrizione delle probabili conseguenze della violazione;
   d. una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.
3. In linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato. In tal caso, si procede a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia .
4. Il Regolamento stabilisce tre condizioni che, se soddisfatte, non richiedono la comunicazione agli interessati in caso di violazione, ossia:
   a. il Titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione, in

particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi.
b. immediatamente dopo una violazione, il Titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche.
c. contattare gli interessati richiederebbe uno sforzo sproporzionato, ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti.

5. Conformemente al principio di responsabilizzazione, il Titolare del trattamento dovrebbe essere in grado di dimostrare all'autorità di controllo di soddisfare una o più delle condizioni di cui al prededente punto 4.
6. L'autorità di controllo qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato può richiedere al Titolare del trattamento di comunicare la violazione all'interessato.

ART. 8 RESPONSABILIZZAZIONE E TENUTA DI REGISTRI

1. Indipendentemente dal fatto che una violazione debba o meno essere notificata all'autorità di controllo, il titolare del trattamento deve conservare la documentazione di tutte le violazioni, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio , annotando la violazione in uno specifico registro che, previa richiesta, deve essere esibito all'autorità di controllo.
2. Al RPD è affidato il compito di tenere il registro di cui al precedente punto 1.
   La mancata corretta documentazione di una violazione può comportare l'esercizio da parte dell'autorità di controllo dei suoi poteri ai sensi dell'articolo 58 e l'imposizione di una sanzione amministrativa pecuniaria ai sensi dell'articolo 83.

ART. 9 SANZIONI E RESPONSABILITA'

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile del trattamento, a meno che il Titolare o il Responsabile dimostrino che l'evento dannoso non è loro in alcun modo imputabile.
2. Il Regolamento stabilisce che la violazione degli obblighi del Titolare e del Responsabile del trattamento è soggetta a sanzioni amministrative pecuniarie.
3. Fatti salvi i poteri correttivi delle Autorità di controllo (art.58, paragrafo 2, del Regolamento) ogni Stato Membro può prevedere norme che dispongono se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche ed organismi pubblici istituiti in tale Stato Membro.

ART.10 RIFERIMENTI NORMATIVI

1. Decreto Legislativo 10 agosto 2018 n, 101 "Disposizioni per l'adeguamento della Normativa Nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione

delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)".

2. Regolamento (UE) 2016/679 del Parlamento Europeo del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in particolare gli articoli 33 (Notifica all'Autorità di Controllo), 34 (notifica agli interessati) e 28 (Responsabile del trattamento).
3. D.Lgs. 196/2003 Codice per la protezione dei dati personali e smi.
4. Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679.
5. Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015.
6. D.Lgs. 82/2005 Codice dell'Amministrazione Digitale (CAD).
7. Provvedimento del Garante sulla notifica delle violazione dei dati personali (data breach) del 30/07/2019.

ART. 11 ALLEGATI

1. Allegato 1) esempi di violazione dei dati.
2. Allegato 2) diagramma di flusso gestione violazione dati.
3. Allegato 3) diagramma di flusso notifica

ART. 12 INDICE DI REVISIONE

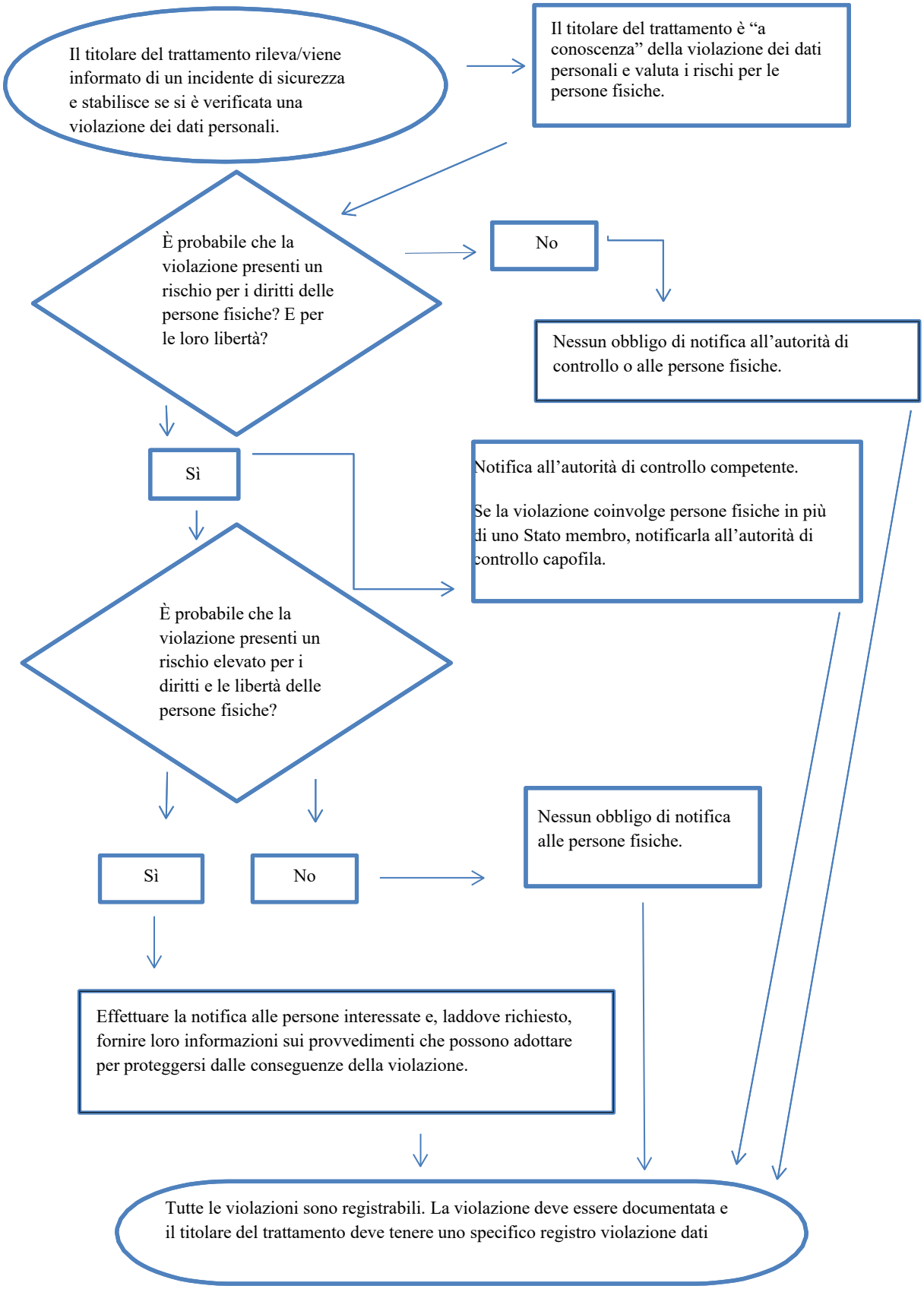
1. La revisione si effettua per intervenute modifiche normative, per cambiamenti assetti organizzativi e per successive valutazioni corredate di adeguate e sostanziali motivazioni

Revisione n°	Data emissione	Tipo modifica	titolo
0	29/01/2020	Prima emissione	

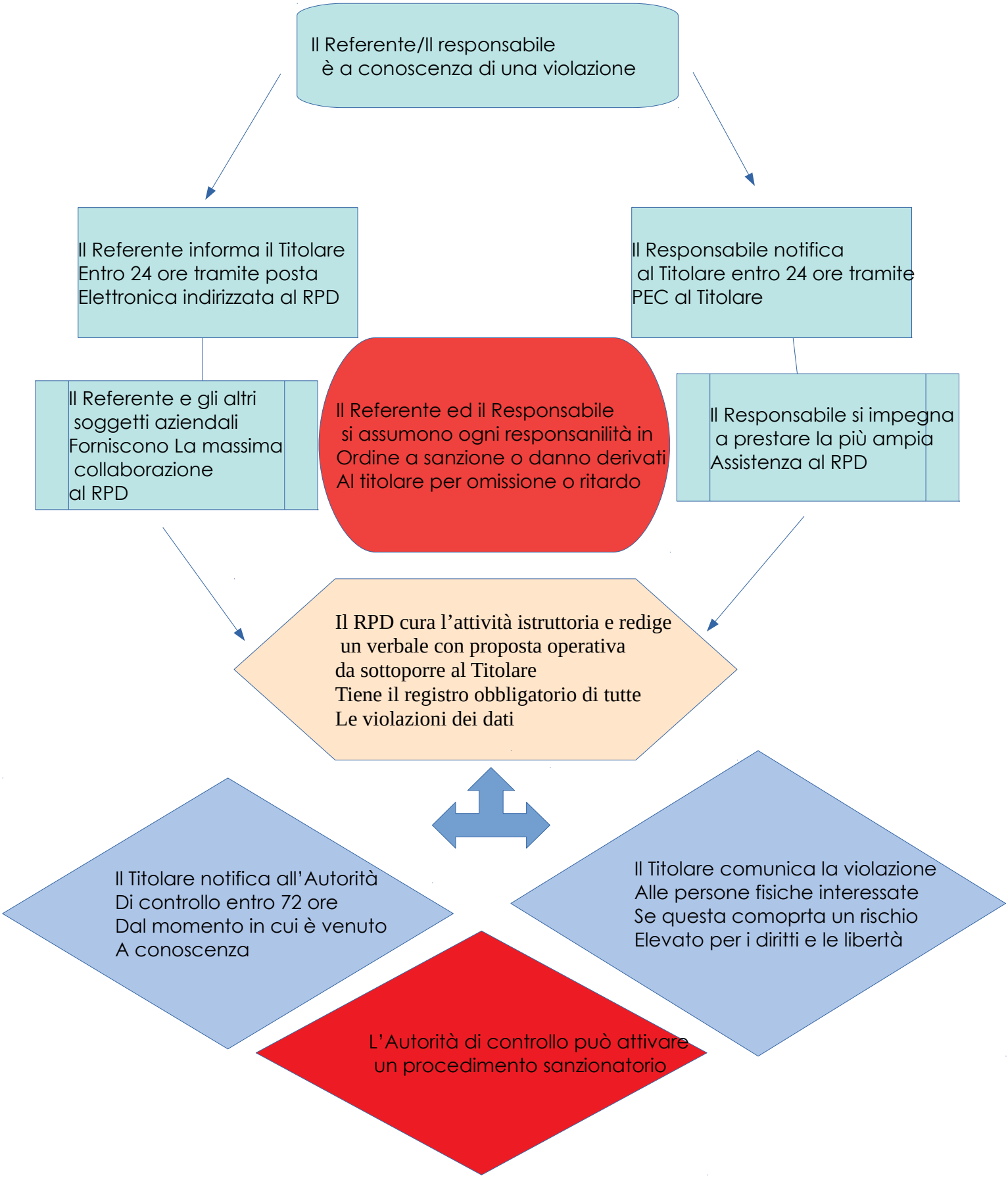
ART. 13 LISTA DI DIFFUSIONE

1. Tutto il personale con ruolo di "incaricato del trattamento dei dati" dell'Azienda USL Toscana Centro mediante inserimento della procedura sulla rete intranet - Portale della Privacy - sezione "Cruscotto".
2. Tutti i Direttori di struttura organizzativa e altro personale con ruolo di "Referente del trattamento dei dati" mediante comunicazione email.
3. Tutti i soggetti esterni con ruolo di Responsabili del trattamento dei dati ex art.28 del GDPR 2016/679, mediante comunicazione nelle forme ritenute adeguate da parte dei soggetti aziendali che hanno designato il soggetto esterno come responsabile del trattamento dei dati.

Sub-Allegato 3: Diagramma di flusso che illustra gli obblighi di notifica



Sub-Allegato 2 Diagramma di flusso che illustra la procedura di gestione di una violazione dei dati



Sub-Allegato 1 Esempi di violazioni dei dati personali e dei soggetti a cui notificarle

Esempio	Notifica all'autorità di controllo?	Comunicazione all'interessato?	Note/raccomandazioni
Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una periferica USB. La chiave viene rubata durante un'effrazione.	No.	No.	Ove i dati siano protetti e crittografati con un algoritmo all'avanguardia, ovvero siano presenti backup dei dati, e la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati. Il titolare del trattamento ha clienti in un solo Stato membro.	Sì, segnalare l'evento all'autorità di controllo se vi sono probabili conseguenze per le persone fisiche.	Sì, segnalare l'evento alle persone fisiche a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per tali persone è elevata	

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