INDICE

N° Cap. Titolo pag.

MODIFICHE RISPETTO ALLA PRECEDENTE REVISIONE (N°.....del _______)

Capitolo\Paragrafo	**Pagina**	**Tipo-natura della modifica**

Redazione			**Verifica e Approvazione**			**Autorizzazione**		
Funzione	Nome e Cognome	Firma	Funzione	Nome e Cognome	Firma	Funzione	Nome e Cognome	Firma
Dirigente UO Affari Generali e Legali	Daniela Righetti	F.to digitalmente	Direttore UO Affari Generali e Legali	Patrizia Casadio	F.to digitalmente	Direttore Amministrativo	Agostina Aimola	F.to digitalmente
Collaboratore esperto amm.vo UO Affari generali e Legali	Patrizia Miserocchi	F.to digitalmente	Responsabile Protezione dei dati	Valeria Mignatti	F.to digitalmente			
			Direttore UO Governo Sistemi Informativi	Paolo Mosna	F.to digitalmente			
			Direttore UO Innovazione e Valutazione delle Tecnologie	Roberto Camillini	F.to digitalmente			

Verifica di conformità		**Rivalidazione**	
Timbro e Firma		**Data**	**Timbro e Firma**
Nunzia Boccaforno F.to digitalmente			

1. OGGETTO/SCOPO

1.1 Oggetto

L'oggetto di questa procedura è la corretta gestione degli incidenti di sicurezza (c.d. *data breach*) che comportino in modo accidentale o in modo illecito la violazione dei dati personali ai sensi del Regolamento UE 679/2016.

Ai fini della presente procedura (policy), una violazione di dati (Data Breach) è considerata qualsiasi violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dall'Azienda della Romagna.
Alcuni esempi di incidenti che determinano ipotesi di violazione possono riguardare:

a) la perdita o il furto di documenti cartacei contenenti dati;
b) la perdita o il furto di apparecchiature informatiche (ad es. PC e laptop), dispositivi mobili (ad es. smartphone o tablet) e strumenti utilizzati per la memorizzazione di dati portatili (ad esempio Hard-disk o chiavette USB) o altri dispositivi contenenti dati;
c) guasti o manomissioni delle apparecchiature;
d) accessi ai locali, o inadeguati controlli sugli accessi, che consentano l'accesso, l'uso o la modifica non autorizzati ai dati trattati;
e) la divulgazione non autorizzata di dati;
f) errori umani (ad es. l'invio di e-mail al destinatario sbagliato);
g) circostanze impreviste quali incendi o allagamenti;
h) episodi di pirateria informatica, come virus, phishing, intercettazioni che mirino ad accedere ai dati con l'inganno, o a comprometterne l'integrità o la disponibilità.

A seconda dei casi, una violazione dei dati personali può incidere su:

- **la riservatezza**, in caso di divulgazione dei dati personali o accesso agli stessi non autorizzato o accidentale;
- **l'integrità**, in caso di modifica non autorizzata o accidentale dei dati personali;
- **la disponibilità**, in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Risulta evidente che una violazione può riguardare contemporaneamente le tre casistiche, nonché qualsiasi combinazione delle stesse.

1.2 Scopo

La presente procedura stabilisce gli obblighi dell'Azienda in qualità di Titolare del trattamento dei dati, in merito alla gestione e alla segnalazione dei Data Breach in conformità al Regolamento UE 2016/679 ("GDPR"). Infatti, lo scopo è stabilire un flusso di attività da implementare in presenza di ipotesi di violazione dei dati personali.

2. CAMPO DI APPLICAZIONE

La presente procedura si applica a tutti i dati raccolti, conservati ed elaborati dall'Azienda USL della Romagna, i quali devono essere gestiti in conformità con le politiche di protezione dei dati stabilite, e mettendo in atto idonee procedure per l'individuazione, l'investigazione e la segnalazione di violazioni dei dati.
In particolare, si applica a tutte le violazioni dei dati, siano esse sospette o confermate, ed è concepita per indicare ai soggetti implicati la corretta gestione di tali violazioni, per determinare se e come devono essere

segnalate:

- al Titolare (nel caso di trattamenti effettuali sia all'interno dell'Azienda sia da parte dei Responsabili (esterni) del trattamento;
- all'autorità competente (Garante per la Protezione dei Dati Personali);
- agli interessati del trattamento.

Per quanto non previsto in questo documento, si richiamano nel loro complesso le norme di legge ed in particolare il Regolamento UE 679/2016.

3. DEFINIZIONI ED ABBREVIAZIONI

DATI PERSONALI: qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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 (Art. 4.1 GDPR).

Rientrano nella categoria di dato personale, ad esempio, documenti di identità, rubriche e-mail, numeri di telefono, coordinate bancarie ecc.
Vanno considerati dati personali anche quei dati che, pur non identificando automaticamente una persona, permettono l'identificazione attraverso confronto con altre fonti di dati, come targhe automobilistiche, indirizzi IP, MAC-address di dispositivi informatici ecc.

CATEGORIE PARTICOLARI DI DATI PERSONALI: dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (Art. 9 del GDPR).

Rientra nelle categorie particolari di dati personali, ad esempio, qualsiasi dato riferito ad un soggetto da cui si possa evincere: lo stato di gravidanza, infortuni, l'iscrizione a un sindacato, l'assenza dal lavoro per motivi religiosi, l'autenticazione tramite riconoscimenti delle impronte digitali, la firma grafometrica ecc.

DATI GIUDIZIARI: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (Art. 10 GDPR).

Sono qualificabili come dati giudiziari, ad esempio, penali di condanna definitivi concernenti le pene accessorie, le informazioni riportate sul casellario giudiziale, misure alternative alla detenzione che hanno prosciolto l'imputato, DASPO ecc.
In termini di precauzioni nei trattamenti, i dati giudiziari devono essere trattati analogamente alle categorie particolari di dati personali.

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 (Art. 4.2 GDPR).

In altri termini, qualunque operazione effettuata sul dato si configura come trattamento.

INTERESSATO: la persona fisica cui si riferiscono i dati personali.

Esempi di interessati: clienti, potenziali clienti, dipendenti, candidati all'assunzione, pazienti, scolari o studenti, utenti di un sito web, soggetti iscritti a un servizio (ad es. newsletter) ecc.

TITOLARE DEL TRATTAMENTO: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (Art 4.7 GDPR).

Quindi, con Titolare del trattamento si fa riferimento all'Azienda della Romagna complessivamente intesa.

RESPONSABILE DEL TRATTAMENTO: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (Art. 4.8 GDPR).
I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico che vincola il Responsabile al Titolare del trattamento, determinandone l'oggetto e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento (Art. 28.3 GDPR).

Si tratta principalmente delle aziende fornitrici che trattano dati necessari a fornire specifici servizi all'Azienda della Romagna, come società informatiche (che abbiano accesso ai dati personali presenti sul sistema informatico), consulenti del lavoro (che trattano dati personali dei dipendenti), altre società coinvolte nell'attività dell'Azienda della Romagna (che accedono ai dati personali dei clienti).

AUTORIZZATO: la persona fisica che ha accesso a dati personali e agisce sotto l'autorità del Titolare o del Responsabile del trattamento, ed è stato istruito a trattarli (Art. 29 GDPR).

Quindi, tutti i dipendenti o collaboratori che trattano dati per l'Azienda USL della Romagna.

GRUPPO DATA BREACH (GDB): il Gruppo aziendale preposto alle analisi sulle segnalazioni dei Data Breach, finalizzate ad offrire al Titolare del trattamento gli elementi di valutazione sulle determinazioni da assumere circa l'incidente di sicurezza occorso. Il Gruppo Data Breach ha la seguente composizione:

- Direttore. U.O. Governo Sistemi Informativi – Coordinatore;
- Responsabile della Protezione dei dati (DPO) Ausl Romagna;
- Direttore U.O. Innovazione e valutazione delle tecnologie;
- Incarico di funzione "Privacy" /Dirigente U.O. Affari Generali e Legali.

4. DESCRIZIONE ATTIVITA' E RESPONSABILITA'

4.1 Matrice delle Responsabilità

Figure responsabili **(Macro)Attività**	Delegato al trattamento	Responsabile esterno del trattamento	Gruppo Data breach GDB.	DPO	Referente Privacy	UO AFFARI GENERALI E LEGALI	Altre UU.OO. Competenti	Direzione Aziendale
Invio Segnalazione data breach	R	R						
Presa in carico segnalazione data breach			R		I			
Contenimento del danno e valutazioni iniziali	C	C	R				C	I
Valutazione del dettaglio di rischio e stima del rischio per gli interessati	C	C	R			C	C	I
Comunicazione alla Direzione Aziendale degli esiti della valutazione sul Data Breach		I	R(coordinatore del Gruppo Data Breach)		I			I
Determinazioni in merito alla notifica all'autorità di Controllo sulla base delle risultanze del Gruppo Data Breach				C		C		R
Notifica all'Autorità di Controllo					R (per delega del Titolare)	R (nei casi di assenza del Referente privacy)		
Valutazione notifica agli interessati			R			C		I
Eventuale comunicazione agli interessati	I	I	C	C		R		I
Aggiornamento del Registro delle violazioni				C		R		

R= Responsabile
C= Collabora
I = Informato

4.2 VIOLAZIONI DI DATI PERSONALI (DATA BREACH) Percorso applicativo IN AZIENDA

Il GDPR definisce la violazione di dati personali (Data Breach) «*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*»; come precisato nel Considerando 85 del GDPR, un Data Breach, se non affrontato in modo adeguato e tempestivo, può provocare danni fisici,

materiali o immateriali alle persone fisiche, quali ad esempio:

- perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti;
- discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale;
- altri danni economici o sociali significativi alla persona fisica interessata.

Il GDPR stabilisce pertanto l'obbligo di segnalare alcuni tipi di violazione dei dati personali direttamente all'autorità di controllo, informando inoltre i singoli interessati nel caso di violazioni che comportino un elevato rischio sui loro diritti e sulle loro libertà. Va osservato che la mancata segnalazione di una violazione a una persona fisica o all'Autorità di controllo può comportare l'imposizione di una sanzione al Titolare del trattamento ai sensi dell'Art. 83 del Reg. (UE) 2016/679.

4.2.1 PRESA DI COSCIENZA E SEGNALAZIONE

Ogni operatore aziendale autorizzato a trattare i dati personali, che accerti un incidente che possa comportare una violazione dei dati personali trattati, o che riceva comunicazione di incidente da un soggetto esterno (individuo o organizzazione), deve darne IMMEDIATA comunicazione al Delegato al trattamento a cui afferisce (di norma il Direttore o il responsabile della struttura presso cui presta servizio).
Questi, valutato puntualmente l'evento, se confermate le valutazioni del potenziale Data Breach, lo segnala tempestivamente utilizzando il report di comunicazione interna (MRPA208 01) **al *Gruppo Data Breach* (GDB)**, attraverso l'indirizzo e-mail: databreach@auslromagna.it**.**
Il gruppo effettua una prima valutazione dell'evento per accertarsi che l'incidente di sicurezza si sia effettivamente verificato, avvalendosi eventualmente di altri contributi secondo le varie competenze aziendali. Se uno dei componenti del GDB viene direttamente a conoscenza anche informalmente del potenziale caso di Data Breach deve far attivare la procedura indicata.

La comunicazione, oltre che tempestiva, deve includere tutti i dettagli noti sull'incidente. A titolo esemplificativo, ma non esaustivo, si indicano:

- l'ora e la data della violazione;
- l'ora e la data in cui è stata scoperta la violazione;
- una descrizione del tipo di violazione accertata (sulla riservatezza, l'integrità o la disponibilità dei dati) o degli elementi per cui si sospetta una violazione;
- le tipologie di dati coinvolti nella violazione (avendo cura di evidenziare eventuali violazioni su categorie particolari di dati personali, o su dati giudiziari);
- le categorie di interessati a cui i dati personali si riferiscono;
- se noto, il numero di interessati coinvolti;
- se note, le modalità con cui è avvenuta la violazione, avendo cura di evidenziare se la violazione è ancora in corso;
- soggetti terzi (ad es. fornitori) qualora coinvolti o direttamente interessati alla violazione;
- le azioni già intraprese per porre rimedio alla violazione.

Qualora l'istruttoria abbia esito positivo, il Titolare del Trattamento viene informato dal GDB. Al fine di stabilire le tempistiche per la gestione del Data Breach, infatti, nelle Linee Guida emendate in data 06.02.2018 dal Gruppo di lavoro europeo sulla notifica delle violazioni dei dati personali è indicato che il Titolare del trattamento deve considerarsi "a conoscenza" di una violazione nel momento in cui è ragionevolmente certo

che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali. Il momento esatto dipenderà dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall'inizio, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi.

4.2.2 CONTENIMENTO DEL DANNO E VALUTAZIONI INIZIALI

È opportuno che la Fase 2 sia realizzata **entro 24 h** dalla presa di coscienza dell'incidente, al fine di minimizzarne gli effetti.
Spetta al GDB stabilire il momento in cui sia opportuno coinvolgere la Direzione Aziendale, sulla base del grado di certezza della violazione, della gravità del possibile impatto, della necessità di attivare specifiche misure di contenimento, o di assumere ulteriori provvedimenti ritenuti necessari.

Al ricevimento di una segnalazione di violazione, il GDB dovrà innanzitutto valutare, con il supporto delle Unità Operative competenti per la trattazione del caso specifico, se la violazione dei dati è ancora in corso e, in tal caso, dovrà indicare le misure appropriate da prendere immediatamente nel caso si ritenga necessario minimizzare o fermare gli effetti della violazione dei dati (ad es., nella misura ragionevolmente praticabile, richiedendo la modifica, limitazione, o revoca delle autorizzazioni di accesso ai dati informatici, o rendendoli temporaneamente non disponibili).

4.2.3 VALUTAZIONE DEL DETTAGLIO DI RISCHIO E STIMA SUL RISCHIO PER GLI INTERESSATI

La Fase 3 deve essere realizzata **entro 48 h** dalla presa di coscienza dell'incidente, al fine di garantire i tempi tecnici per inviare l'eventuale notifica al Garante.

Il GDB, avvalendosi delle unità operative competenti e di altre professionalità ritenute necessarie per il caso specifico, effettuerà una valutazione della violazione dei dati. Nello specifico, dovranno essere raccolte (o verificate e confermate, se già riportate nella comunicazione di cui alla Fase 1) tutte le informazioni volte a valutare il rischio per i soggetti interessati. In particolare:

- Tipologia del breach (riservatezza, integrità, disponibilità);
- Natura, criticità e volume dei dati coinvolti dal data breach;
- Facilità di identificazione degli interessati;
- Criticità delle conseguenze per gli interessati;
- Numero degli interessati coinvolti dal data breach;
- Caratteristiche del Titolare dei dati oggetto del data breach;

In tale Fase, possono inoltre essere tenuti in considerazione altri elementi rilevanti, ad esempio:

- eventuali obblighi legali o contrattuali di notifica;
- l'applicazione di misure a protezione dei dati interessati (come la pseudonimizzazione o la crittografia), che rendano quindi i dati inutilizzabili a qualsiasi parte non autorizzata.

Una volta completate le indagini, il GDB tiene informata la Direzione Aziendale in merito alla individuazione dei soggetti a cui dovrà essere notificata la violazione. La valutazione del dettaglio di rischio viene effettuata utilizzando il Tool per la valutazione del rischio associato al Data Breach, progettato con l'obiettivo di fornire in output il livello di rischio privacy sui soggetti interessati a valle di una violazione e basato sulla metodologia realizzata da ENISA (European Union Agency for Network and Information Security). Allo scopo di valutare il rischio, il Tool presenta delle domande funzionali a determinare il livello di impatto privacy relativo alla violazione. Le risposte sono guidate dal documento stesso e sono pesate sulla base della gravità del Data Breach e gli eventuali adempimenti correlati rispetto alla notifica e alla comunicazione agli interessati.
In ogni caso, i risultati dell'analisi del Data Breach svolta attraverso il Tool, così come qualsiasi altra considerazione sul caso, dovranno essere documentati, conservati e archiviati presso l'U.O. Affari Generali e Legali.

Qualora il Tool ENISA dia esito: *"Da verificare*", compete al GDB, tramite il Coordinatore del medesimo, proporre al Titolare del trattamento, attraverso una relazione, gli elementi di valutazione in merito alla decisione di notificare o meno il Data Breach. Il Titolare del trattamento assume le determinazioni conseguenti provvedendo in merito alla notifica o soprassedendovi, in esito al giudizio di probabilità che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, secondo le risultanze emerse.

4.2.4 NOTIFICA ALL'AUTORITÀ DI CONTROLLO

A meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento ha l'obbligo di notificare la violazione all'Autorità di controllo competente senza ingiustificato ritardo. Qualora tale notifica sia effettuata oltre il limite delle 72 ore, deve essere corredata dei motivi del ritardo.
È compito del Referente Privacy aziendale, in virtù di delega conferita dal Direttore Generale, sulla base delle valutazioni di cui ai punti precedenti e con la supervisione del DPO, provvedere alla redazione e invio della notifica seguendo il Modello telematico indicato dall'Autorità Garante.

La notifica deve riportare almeno:

- 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;
- il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere maggiori informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate, o di cui si propone l'adozione, da parte del Titolare del trattamento per porre rimedio alla violazione e, se del caso, per attenuarne i possibili effetti negativi.

All'atto della notifica all'Autorità di controllo, il Titolare del trattamento può ottenere dalla stessa Autorità di controllo consulenza sull'eventuale necessità di informare le persone fisiche interessate. Una volta effettuata la notifica, sarà compito del DPO mantenere i rapporti e i contatti con l'Autorità, supportandola in ogni operazione, attività o indagine, e rispettando tutte le eventuali indicazioni da questa ricevute, fino alla chiusura del procedimento. Dovrà altresì mantenere regolarmente informata e aggiornata la Direzione Aziendale rispetto alla natura di tutte le operazioni e sull'esito del procedimento di notifica (ad es. prescrizioni, sanzioni ecc.).

4.2.5 COMUNICAZIONE ALL'INTERESSATO

Quando la violazione potrebbe comportare un elevato rischio per i diritti e le libertà dell'interessato è necessario informarlo (in un tempo ragionevole e secondo le direttive dell'Autorità di controllo).

Oltre all'esito della valutazione di cui alla Fase 3, può risultare un utile riferimento l'Allegato B delle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679 emendate in data 06.02.2018, dove è riportata una lista di esempi in cui si può considerare che la violazione comporti un alto rischio per l'interessato.

Il Titolare del trattamento, ove possibile, dovrebbe contattare tutti gli interessati; se tale operazione implica uno sforzo sproporzionato, è invece possibile procedere con una comunicazione pubblica, ad esempio tramite banner e notifiche messe in evidenza sul sito web o annunci sulla stampa.
I contenuti della comunicazione sono definiti dall'Articolo 34 del Reg. (UE) 2016/679, secondo cui devono essere riportati almeno:

- una descrizione della natura della violazione;
- il nome e le coordinate di contatto del DPO o di un altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;

- una descrizione delle misure prese o proposte per gestire la violazione e, ove possibile, le misure appropriate per mitigare le possibili conseguenze negative.

Ulteriori e opportuni elementi da valutare nello svolgimento della comunicazione sono:

- eventuali considerazioni particolari applicabili a determinate categorie di soggetti interessati (come minori o persone vulnerabili);
- i modi per agevolare le persone coinvolte nella violazione di dati nel contattare il Titolare per ottenere maggiori informazioni sulla violazione dei dati;
- l'ulteriore assistenza che l'Azienda dovrebbe fornire agli interessati, ove opportuno.

Pertanto, successivamente alla decisione di notifica all'Autorità Garante, il GDB valuta l'opportunità/necessità di notifica agli interessati, all'esito della valutazione circa la potenzialità del rischio di lesività dei diritti correlati. Se dalle valutazioni fatte con le modalità di cui ai punti precedenti emerge la necessità di notifica agli interessati, l'UO Affari Generali e Legali, predispone la conseguente comunicazione, a firma del Titolare da inviare nei tempi e nei modi che lo stesso, anche attraverso la funzione consulenziale del DPO, individuerà come più opportuna tenendo anche conto di eventuali indicazioni fornite dall'Autorità Garante. La comunicazione descriverà con un linguaggio semplice e chiaro la natura della violazione dei dati personali, le probabili conseguenze della stessa, nonché le misure individuate per il rimedio.

Tutte le operazioni e attività realizzate per la comunicazione agli interessati (ad es. contratti con società terze sull'invio di sms/e-mail, copia dell'articolo di giornale, report, ecc.), compresa la comunicazione agli interessati, è conservata e archiviata presso l'UO Affari Generali e Legali.

4.2.6 GESTIONE DEL PROCESSO DEL DATA BREACH DA PARTE DEL RESPONSABILE DEL TRATTAMENTO

Ogni qualvolta l'Azienda si trovi ad affidare il trattamento di dati a un soggetto terzo/responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati.
A tal fine è necessario che la presente procedura di segnalazione di Data Breach sia resa nota a tutti i Responsabili del trattamento con l'obiettivo di fornire le istruzioni per informare il titolare del trattamento, senza ingiustificato ritardo, di ogni potenziale evento di Data Breach.

Pertanto il Responsabile del trattamento, qualora venga a conoscenza di un potenziale caso di Data Breach, deve avvisare, senza ingiustificato ritardo e nel rispetto dei tempi previsti nell'atto di nomina, l'Azienda USL della Romagna all'indirizzo PEC: azienda @pec.auslromagna.it o tramite raccomandata A/R all'indirizzo Via De Gasperi, 8 – Ravenna o al DPO con e-mail : dpo@auslromagna.it , utilizzando il report per la segnalazione di un sospetto caso di Data Breach (MRPA208 02).
Da questo momento vengono eseguiti i medesimi step della procedura illustrata al paragrafo 5.

4.2.7 REGISTRO DELLE VIOLAZIONI

Il Regolamento UE n. 679/2016 prescrive al Titolare del trattamento dei dati di documentare qualsiasi violazione di dati personali, al fine di consentire all'Autorità di Controllo di verificare il rispetto della norma.
Pertanto, come previsto nella PA 262, l'UO Affari Generali e Legali aggiorna e conserva il Registro delle violazioni dei dati personali secondo le indicazioni fornite dal DPO.

5. DOCUMENTI DI RIFERIMENTO

- 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 (di seguito anche solo GDPR): Articoli 33 e 34; Considerando 85;

- 18/IT WP250 – LINEE GUIDA SULLA NOTIFICA DELLE VIOLAZIONI DEI DATI PERSONALI AI SENSI DEL REGOLAMENTO (UE) 2016/679 adottate il 3 ottobre 2017 emendate il data 06.02.2018;
- PA 262 "Procedura in materia di protezione dei dati personali e organigramma Privacy" adottata con deliberazione n.347 del 27.10.2021.
- Tool per la valutazione del rischio associato al Data Breach (ENISA)

6. DOCUMENTI COLLEGATI

MRPA208 01: Modulo di segnalazione di violazione;
MRPA 208 02: Modello di segnalazione di violazione da parte del responsabile del trattamento.

7. MODALITA' DI VERIFICA E CONTROLLO

Dalla gestione di un Data Breach scaturiscono una serie di azioni di seguito riportate utili al miglioramento del processo:

- Analisi della relazione dettagliata sull'incidente;
- Eventuale revisione della presente procedura e di eventuali altri documenti collegati (es. Analisi del rischio, Misure di sicurezza);
- Individuazione di controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
- Revisione delle relazioni con Clienti e Fornitori.

Al fine di verificare la corretta applicazione della gestione delle segnalazioni di data Breach si individua la seguente modalità di controllo:

INDICATORE	STANDARD	PERIODICITA' DI RILEVAZIONE	RESPONSABILITA' DI RILEVAZIONE
Numero di notifiche al Garante rispetto al numero di violazioni	In diminuzione rispetto all'anno precedente	Annuale	Referente privacy
Numero di comunicazioni agli interessati rispetto al numero di violazioni rischio alto	In diminuzione rispetto all'anno precedente	Annuale	UO AFFARI GENERALI E LEGALI

8. DISTRIBUZIONE E DIFFUSIONE

Il testo del presente documento è messo a disposizione di tutto il personale dell'Azienda mediante inserimento nell'apposita sezione della Rete Intranet Aziendale con comunicazione via mail a tutti gli operatori dell'AUSL della Romagna e inserimento nel bollettino periodico, inoltre è pubblicata nel sito internet: https://amministrazionetrasparente.auslromagna.it/pubblicita-legale/privacy-tutela-dati-personali.
Inoltre, la presente è inviata con nota protocollata a:
- Direttori di Presidio Ospedaliero
- Direttori dei Dipartimenti
- Direttori Piattaforme Amministrative
- Direttori dei Distretti sanitari
- Direttori delle UU.OO. di staff.

I responsabili (esterni) del trattamento dei dati saranno informati mediante inserimento di clausola apposita nel contratto di nomina a responsabile del trattamento, con indicazione del link di collegamento alla presente procedura.