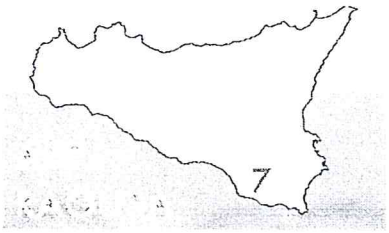

Titolare del trattamento : Azienda Sanitaria Provinciale di Ragusa

Data Protection Officer (D.P.O.): Dott.ssa Giovanna Di Stefano

Procedura sulla gestione delle violazioni di dati personali

(Data Breach)

INFORMAZIONI DOCUMENTO:

Titolo	Procedura sulla gestione delle violazioni di dati personali (Data Breach)		
Data di emissione	_____	**Versione**	1.0

SOMMARIO

I INTRODUZIONE

A. SCOPO

La presente Procedura sulla gestione delle violazioni di dati personali (nel prosieguo definite anche "Data Breach") ha lo scopo di fornire le indicazioni pratiche della Azienda in caso di Violazione dei Dati Personali, nel rispetto della normativa in materia di trattamento dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento EU 2016/679. In questo documento si sintetizzano le regole per garantire il rispetto dei principi esposti nonché la realizzabilità tecnica e la sostenibilità organizzativa, nella gestione del *data breach*, sotto i diversi aspetti relativi a:

- modalità e profili di segnalazione al Titolare
- modalità e profili di segnalazione all'Autorità Garante
- valutazione dell'evento accaduto
- eventuale comunicazione agli interessati

B. CAMPO DI APPLICAZIONE

La presente procedura si applica all'Azienda Sanitaria Provinciale di Ragusa, nella qualità di Titolare del trattamento, nonché alla Società/Ditta designata Responsabile del trattamento

C. NORMATIVA DI RIFERIMENTO

Regolamento EU 2016/679 considerando n. 85, 86, 87, 88 artt. 33, 34

Art. 33. Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il Responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

2.La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del Responsabile della protezione dei dati- Data Protection Officer;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

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

5.Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34 -Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

D. GLOSSARIO E ACRONIMI

Archivio: qualsiasi insieme strutturato di Dati Personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Aree Sensibili: sono quei luoghi fisici o della Rete in cui vengono Trattati Dati Particolari e/o Dati Giudiziari relativi a persone fisiche; e/o luoghi in cui vengono gestiti e consultati documenti riservati a cui è assolutamente vietato accedere se non per motivi di servizio.

Autorità di Controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR;

Consenso dell'Interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati Personali che lo riguardano siano oggetto di Trattamento;

Dati Biometrici: i Dati Personali ottenuti da un Trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati Comuni: sono tutti i Dati Personali che non appartengono alle categorie dei Dati Particolari e Dati Giudiziari;

Dati Genetici: i Dati Personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

Dati Giudiziari: Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;

Dati Particolari: Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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;

Dati relativi alla Salute: i Dati Personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

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;

Destinatario/i: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di Dati Personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di Dati Personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate Destinatari; il Trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del Trattamento;

Dispositivi Fissi: si intendono gli strumenti informatici non facilmente removibili dal perimetro aziendale quali personal computer, server locali, stampanti affidati alle Persone Autorizzate per uso professionale;

Dispositivi Mobili: in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, hard disk esterni, tablet e smartphone utilizzati dalla Persone Autorizzate per uso professionale;

DPO o **Data Protection Officer**: è una persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37.1 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;

GDPR o **Regolamento:** Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679.

Delegato e Incaricato o Persona/e Autorizzata/e: 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. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, collaboratori e lavoratori

QO

a partita IVA, part-time, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, nonché consulenti e fornitori dell'Azienda e, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti Aziendali o Strumenti Personali, operino sulla Rete ovvero siano a conoscenza di informazioni aziendali rilevanti quali, a titolo esemplificativo e non esaustivo: (a) i Dati Personali di utenti/clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura finanziaria nonché (c) i dati e le informazioni relative ai processi aziendali.

Limitazione Di Trattamento: il contrassegno dei Dati Personali conservati con l'obiettivo di limitarne il Trattamento in futuro;

Processo Decisionale Automatizzato: decisione basata unicamente sul Trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona;

Profilazione: qualsiasi forma di Trattamento automatizzato di Dati Personali consistente nell'utilizzo di tali Dati Personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Pseudonimizzazione: il Trattamento dei Dati Personali in modo tale che i Dati Personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile;

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27 GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del GDPR;

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; 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;

Rete: rappresenta il perimetro digitale dell'Azienda contenente Dati Personali e/o informazioni riservate comprensivo della rete interna (intranet) e della rete esterna (internet) .

Strumenti Aziendali: l'insieme di Dispositivi Fissi e Dispositivi Mobili concessi in comodato d'uso dall'Azienda alle Persone Autorizzate al fine di svolgere le proprie mansioni;

Strumenti Personali: i Dispositivi Mobili di proprietà delle Persone Autorizzate autorizzati ad essere impiegati per uso professionale;

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del Trattamento, il Responsabile del Trattamento e le Persone Autorizzate al Trattamento dei Dati Personali sotto l'autorità diretta del Titolare o del Responsabile;

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 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;

Violazione Dei Dati Personali ovvero **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.

Si possono distinguere tre tipi di violazioni:

- Violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
- Violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
- Violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali (un incidente che determini la non disponibilità di dati per un periodo di tempo deve essere comunque considerato violazione).

II. FASE 1: RACCOLTA DELLE INFORMAZIONI

A CANALI INTERNI

Le segnalazioni interne di eventi anomali possono:

- pervenire dal personale dell'Azienda

- essere inoltrate dal D.P.O.

B CANALI ESTERNI

Le segnalazioni possono pervenire anche da fonti esterne, o anche dall'analisi di informazioni presenti sul Web, ovvero dai Responsabili del trattamento.

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.

Le segnalazioni, a qualunque soggetto/funzione pervengano, devono essere tempestivamente comunicate al D.P.O., comunque **non oltre 12 ore** dalla conoscenza della violazione, ove possibile a mezzo PEC, al seguente indirizzo:dpo@asp.rg.it

La presa in carico di tutte le segnalazioni è di responsabilità del D.P.O. che provvederà a gestirle coinvolgendo le altre funzioni interessate secondo quanto specificato nella presente procedura.

III DATA BREACH PRESSO L'AZIENDA IN QUALITÀ DI TITOLARE – FASE 2 - ANALISI DELLE SEGNALAZIONI

A. ANALISI PRELIMINARE E ELABORAZIONE DELLA SCHEDA EVENTO

Il DPO avvia un'analisi preliminare finalizzata alla raccolta dei dati concernenti l'anomalia e alla compilazione della Scheda Evento (all. A) della presente procedura) contenente tutte le informazioni raccolte:

- Data evento anomalo;
- Data presunta di avvenuta violazione;
- Data e ora in cui si è avuto conoscenza della violazione;
- Fonte segnalazione;
- Tipologia violazione e di 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 altresì se essa sia avvenuta a seguito di smarrimento di Dispositivi Mobili;

- 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.

B. ANALISI DI PRIMO LIVELLO - VERIFICA DELLA SEGNALAZIONE

Obiettivo dell'analisi di primo livello è quella di verificare che la segnalazione non si tratti di un cd. "falso positivo". Nel caso la violazione su dati personali venga accertata, il DPO, responsabile dell'analisi di primo livello, con la collaborazione delle direzioni coinvolte dalla violazione, recupera le informazioni di dettaglio sull'evento necessarie 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.

L'evento viene comunque inserito a cura del DPO nel Registro dei Data Breach (all. C) della presente procedura) nella apposita sezione dedicata agli "eventi falsi positivi".

C. ANALISI DI SECONDO LIVELLO - SCHEDA VIOLAZIONE DATI

L'analisi di secondo livello, finalizzata alla valutazione d'impatto, viene effettuata dal Gruppo di lavoro Privacy, coordinato dal D.P.O. e alla presenza del Commissario/Direttore Generale:
Dall' analisi congiunta di tutte le informazioni raccolte si redige una Scheda Violazione Dati (all. B) della presente procedura) per le conseguenti valutazioni.

Il Gruppo di lavoro Privacy classifica l'evento 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 non autorizzata
- accesso ai dati personali illecito.

La violazione deve essere valutata secondo i livelli di rischio:

- NULLO
- BASSO

- ☐ MEDIO
- ☐ ALTO

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.

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

a) che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;

b) che si tratti di dati relativi a valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;

c) che si tratti di dati di persone fisiche vulnerabili, in particolare minori;

d) che il trattamento riguardi una notevole quantità di Dati Personali;

e) che il trattamento riguardi un vasto numero di Interessati.

Il Gruppo di lavoro Privacy deve provvedere affinché vengano tempestivamente adottate misure che consentano di minimizzare le conseguenze negative della violazione.

IV. FASE 3: NOTIFICA E COMUNICAZIONE

A. NOTIFICA ALLA AUTORITÀ DI CONTROLLO

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

Il D.P.O. 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 e dunque sia stato dallo stesso classificato **"NULLO"** .

Qualora la notifica all'Autorità di Controllo non sia effettuata entro 72 ore, va corredata dei motivi del ritardo.

La notifica all'Autorità di Controllo deve:

a) descrivere, ove possibile:
   i. la natura della Violazione dei Dati Personali compresi
   ii. le categorie e il numero approssimativo di Interessati in questione
   iii. le categorie e il numero approssimativo di registrazioni dei Dati Personali in questione;
b) comunicare il nome e i dati di contatto del DPO 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 dell'Azienda per porre rimedio alla Violazione dei Dati Personali e anche, se del caso, per attenuarne i possibili effetti negativi.

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

B. COMUNICAZIONE DELLA VIOLAZIONE ALL'INTERESSATO

Il DPO sentita la Direzione Generale, deve informare gli interessati dell'evento anomalo, in tutti i casi in cui, a norma dell'art. 33-34 GDPR, il Gruppo di lavoro Privacy valuti che la violazione risulta presentare rischi classificati come *"ALTI"* nella Scheda Violazione Dati per i diritti e le libertà delle persone fisiche.

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 effettuata ad opera del Gruppo di lavoro Privacy e deve essere intellegibile, coincisa, trasparente, e facilmente accessibile; deve essere utilizzato un linguaggio semplice e chiaro adottando, se possibile, la stessa lingua parlata dall'Interessato. Rispetto alle modalità della comunicazione si applicano quelle ritenute più idonee dal Gruppo di lavoro Privacy .

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

a) data e ora della violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa;
b) la natura della Violazione dei Dati Personali;
c) il nome e i dati di contatto del DPO;
d) le probabili conseguenze della Violazione dei Dati Personali;
e) la descrizione delle misure adottate o di cui si propone l'adozione da parte dell'Azienda per porre rimedio alla Violazione dei Dati Personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

a) Sono state messe in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai Dati Personali oggetto della violazione, in particolare quelle destinate a rendere i Dati Personali incomprensibili a chiunque non sia autorizzato ad accedervi, **quali la cifratura**; salvo i casi in cui la violazione della sicurezza ha comportato la distruzione o la perdita dei Dati Personali degli Interessati;
b) 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;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia.

L'Azienda riporta in calce un Modello di comunicazione all'Interessato della Violazione dei Dati Personali.

V. FASE 4: REGISTRAZIONE SEGNALAZIONE NEL REGISTRO DEI DATA BREACH

Nel Registro dei Data Breach (all. C) della presente procedura), il D.P.O. documenta ogni singolo evento, sia esso, **FALSO**, **IRRILEVANTE** ovvero **RILEVANTE**; in questi due ultimi 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 D.P.O. sotto la responsabilità dell'Azienda, Titolare del trattamento.

VI. 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 della struttura informatica aziendale, con eventuale supporto da parte di altre aree funzionali.

VII DATA BREACH PRESSO LA SOCIETÀ O UN TERZO IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO

A. OBBLIGHI DI COMUNICAZIONE DELLA SOCIETÀ QUANDO OPERA IN QUALITÀ DI RESPONSABILE

Quando la Società agisce in qualità Responsabile, in caso di Violazione dei Dati Personali, deve informare il Titolare del trattamento, senza ingiustificato ritardo secondo i tempi e i modi concordati nel contratto per il trattamento dei dati personali trasmesso da quest'ultimo

B. OBBLIGHI DI COMUNICAZIONE DI UN RESPONSABILE NEI CONFRONTI DELL'AZIENDA SANITARIA

Quando un terzo agisce in qualità di Responsabile del Trattamento, in caso di Violazione dei Dati Personali, deve informare l'Azienda (che agisce in qualità di Titolare), senza ingiustificato ritardo e non al più tardi di 24 ore dal momento in cui ha conoscenza della violazione, inviando una comunicazione ai seguenti indirizzi [ove possibile via PEC]:

- dpo@asp.rg.it
- direzione.generale@pec.asp.rg.it

e successivamente collaborare con l'Azienda per consentirle di adempiere agli obblighi previsti dalla normativa agli artt. 33 e 34 GDPR. La procedura che segue è riportata come allegato nel Contratto per il Trattamento dei Dati Personali, salvo diversamente concordata con il Responsabile.

Il Responsabile deve assistere l'Azienda avviando un'analisi preliminare finalizzata alla raccolta dei dati concernenti l'anomalia e alla compilazione della Scheda Evento utilizzando il modello allegato alla presente procedura, contenente tutte le informazioni raccolte:

- Data evento, anche la data presunta di avvenuta violazione (in tal caso va specificato)
- Data e ora in cui si è avuto conoscenza della violazione;
- Fonte segnalazione;
- Tipologia violazione e di informazioni coinvolte;
- Descrizione evento anomalo;
- Numero interessati coinvolti;
- Numerosità di dati personali di cui si presume una violazione;
- Indicazione della data, anche presunta, della violazione e del momento in cui se ne è avuta conoscenza;
- Indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di Dispositivi Mobili;
- Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

Una volta condotta l'analisi preliminare, il Responsabile deve condurre un'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 alla Azienda agli stessi indirizzi di cui sopra, al fine di consentirle di inserire l'evento nella sezione "eventi falsi positivi" del Registro dei Data Breach (all. C).

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 D.P.O..

L'evento deve essere inserito dall'Azienda in un apposito Registro dei Data Breach il cui modello è allegato alla presente procedura.

L'Azienda, una volta ricevuta la Scheda Evento deve procedere secondo le prescrizioni di cui ai paragrafi III.C; IV; V e VI della presente procedura.

SCENARI DI DATA BREACH

Di seguito sono illustrati alcuni esempi, non esaustivi, di possibili violazioni di dati personali, allo scopo di supportare i soggetti coinvolti nella procedura, nella valutazione in merito alla necessità di effettua re o meno la notifica di Data Breach

Tipo di Breach	**Definizione**	**Estensione minima o Soglia di segnalazione**	**Esempi**
Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del Titolare, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	• Dati non recuperabili o provenienti da procedure non ripetibili. Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Rottura di un apparecchio elettro-medicale prima di inviare al sistema centrale il dato (immagine, valori, ecc). • Guasto non riparabile dell'hard disk contenente uno o più referti che erano salvati localmente. • Incendio di archivio cartaceo delle cartelle cliniche. • Distruzione di campioni biologici. <u>NON RIENTRA NELLA CASISTICA:</u> • Rottura di una Pen drive USB che non contiene dati personali originali (in unica copia). • Rottura di un PC che non contiene dati personali originali (in unica copia). • Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo.

Perdita	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del Titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	• Dati non recuperabili o provenienti da procedure non ripetibili. • Dati relativi a più assistiti, relativi a interi episodi o relativi a tipologie di dato la cui indisponibilità lede i diritti fondamentali dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamentali dell'interessato. Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	• Smarrimento di Pen drive USB contenente dati originali. • Smarrimento di fascicolo cartaceo personale dipendente. • Infezione da ransomware che provoca la crittografia di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa chiaro che l'unica funzionalità del ransomware era quella di crittografare i dati e che non c'erano altri malware presenti nel sistema. <u>NON RIENTRA NELLA CASISTICA:</u> • Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa. • Furto di una Pen drive USB contenente dati crittografati. Se i dati sono stati crittografati con un algoritmo avanzato, ed esiste il backup dei dati contenuti nella chiavetta, e la chiave crittografica non è stata compromessa, ed i dati possono essere ripristinati in tempo utile allora non è necessario eseguire la notifica all'autorità.
Modifica	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	• Modifiche sistematiche su più casi. Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Guasto tecnico che altera parte dei contenuti di un sistema clinico, compromettendo anche i backup. • Azione involontaria, o fraudolente, di un utente che porta all'alterazione di dati sanitari in modo non tracciato e irreversibile. <u>NON RIENTRA NELLA CASISTICA:</u> • Guasto tecnico che altera parte dei contenuti di un sistema clinico, rilevato e sanato tramite operazioni di recovery. • Azione involontaria di un utente che porta all'alterazione di dati tracciata e reversibile. • Modifica di un documento non

			ancora validato dal proprio autore.
Divulgazione non autorizzata	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Consegna di un CD con dati dei pazienti ad altra struttura senza autorizzazione. <u>NON RIENTRA NELLA CASISTICA:</u> • Il medico sul proprio sistema dipartimentale seleziona il paziente Mario Rossi ma visita il paziente Luca Bianchi. Inserisce anamnesi e gli altri valori di refertazione. • Infezione virale di un PC con un virus che non trasmette dati su internet. • Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.
Accesso non autorizzato	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal Titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi. • Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema clinico. <u>NON RIENTRA NELLA CASISTICA:</u> • Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi. • Accesso non autorizzato di un documento non ancora validato dal proprio autore.
Indisponibilità temporanea	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato.	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale.	• cancellazione accidentale dei dati da parte di una persona non autorizzata e successivo ripristino da backup. • Le cartelle cliniche non sono disponibili per un periodo di 30 ore a causa di un attacco informatico. <u>NON RIENTRA NELLA CASISTICA:</u> • Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso.

VIII. ALLEGATI

A SCHEDA EVENTO

SCHEDA EVENTO	
CODICE	
Data evento e ora della violazione anche solo presunta (specificando se è presunta);	
Data e ora in cui si è avuto conoscenza della violazione;	
Fonte di segnalazione	
Tipologia evento anomalo	
Descrizione evento anomalo	
Numero interessati coinvolti	
Numerosità dei dati personali di cui si presume la violazione	
Data, anche presunta, della violazione e del momento in cui se ne è avuta conoscenza	

Luogo in cui è avvenuta la violazione dei dati (specificare se è avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)	
Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	

B. SCHEDA VIOLAZIONE DATI

SCHEDA VIOLAZIONE DATI		
CODICE EVENTO[1]	CLASSIFICAZIONE[2]	RISCHIO[3]

1. Inserire il CODICE della scheda evento
2. Il Gruppo di Lavoro classifica l'evento 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 non autorizzata
- accesso ai dati personali illecito.

3. Il Gruppo di lavoro valuta il rischio secondo i seguenti livelli di rischio:

- **NULLO**
- **BASSO**
- **MEDIO**
- **ALTO**

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:

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

C. REGISTRO DEI DATA BREACH

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

C. MODELLO DI COMUNICAZIONE ALL'INTERESSATO DELLA VIOLAZIONE DEI DATI PERSONALI

Secondo quanto prescritto dall'art. 34 del Regolamento Generale in materia di protezione dei dati personali RE (UE) 679/2016, la società_____, titolare del trattamento, con la presente è a comunicarLe, l'intervenuta violazione dei Suoi dati personali (data breach) che si è verificata in data_____, alle ore_____; di cui si è avuto conoscenza in data _____, alle ore_____-DATA

A) Descrizione della natura della violazione:

a) Dove è avvenuta la violazione dei dati?

Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili

b) 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)

c) Dispositivo oggetto di violazione, per esempio:

- Computer
- Rete
- Dispositivo mobile
- Strumento di backup
- Documento cartaceo

d) 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 (user name, 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

Tale violazione è suscettibile di presentare un rischio elevato per Suoi diritti e le libertà;

B) Descrivere le probabili conseguenze della violazione dei dati personali;

C) Descrivere quali sono le misure tecnologiche e 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 del DPO, Dott.ssa Giovanna Di Stefano ai seguenti indirizzi:

- Via G.Di Vittorio, 51- 97100 Ragusa
- dpo@asp.rg.it
- numero telefonico 0932.600739

Data, Luogo _____

Il D.P.O.