Policy sulla gestione delle violazioni di dati personali

INFORMAZIONI DOCUMENTO:

Titolo	Policy sulla gestione delle violazioni di dati personali		
Data di emissione	25/5/2018	**Versione**	1.0

SOMMARIO

I. INTRODUZIONE

A. SCOPO

La presente Procedura sulla gestione delle violazioni di dati personali (nel prosieguo definite anche, al singolare, “Data Breach”) ha lo scopo di fornire le indicazioni pratiche della Società in caso di Violazione dei Dati Personali.
Salvo diversamente previsto all’interno di questo documento, tutti i termini riportati con lettera iniziale maiuscola si riferiscono alle definizioni riportate nel GDPR e riportate per comodità nella sezione “Glossario e Acronimi”.

B. CAMPO DI APPLICAZIONE

La presente procedura si applica alla società Ospedale San Raffaele Srl sia che ricopra la funzione di Titolare (cfr. sezione III) sia quella di Responsabile (cfr. sezione VII)

C. NORMATIVA DI RIFERIMENTO

Articolo 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.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. 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 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.
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 o **Consenso**: 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;

Device 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;

Device Mobili: in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, SD cards, 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.
Gruppo Imprenditoriale: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

Incaricato/i 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, sindaci, collaboratori e lavoratori a partita IVA, lavoratori a chiamata, part-time, *job-sharing*, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, nonché consulenti e fornitori della Società 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 clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura commerciale, finanziaria o di strategia di business; nonché (c) i dati e le informazioni relative ai processi aziendali, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale, la cui tutela prescinde dagli effetti pregiudizievoli che potrebbe comportare la diffusione delle medesime.

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 o **Responsabile**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;

Rete: rappresenta il perimetro digitale della Società contenente Dati Personali e/o informazioni riservate comprensivo della rete interna (intranet) e della rete esterna (internet) a cui ci si può collegare via rete LAN, Wi-Fi o VPN.

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

Strumenti Personali: i Device 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 o **Titolare:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di dati personali; quando le finalità e i mezzi di tale Trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Trattamento o **Trattato/Trattati:** 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;

Trattamento Transfrontaliero: a) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un Titolare del Trattamento o Responsabile del Trattamento nell'Unione ove il Titolare o il Responsabile siano stabiliti in più di uno Stato membro; oppure, b) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare o Responsabile nell'Unione, ma che incide o probabilmente incide in modo sostanziale su Interessati in più di uno Stato membro;

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;

II. FASE 1: RACCOLTA DELLE INFORMAZIONI

A. CANALI INTERNI

Le segnalazioni interne di eventi anomali possono:

- pervenire dal personale della Società;
- essere inoltrate dal DPO, ove esistente.

B. CANALI ESTERNI

Le segnalazioni possono pervenire anche da fonti esterne, o anche dall'analisi di informazioni presenti sul Web, ovvero dai Responsabili] (cfr. sezione VII).

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 DPO comunque non oltre 12 ore dalla conoscenza della violazione, ove possibile a mezzo PEC, al seguente indirizzo: dpo@hsr.it

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

III. DATA BREACH PRESSO LA SOCIETÀ IN QUALITÀ DI TITOLARE – FASE 2 - ANALISI DELLE SEGNALAZIONI

A. ANALISI PRELIMINARE E ELABORAZIONE DELLA SCHEDA EVENTO

La DBAU avvia un'analisi preliminare finalizzata alla raccolta dei dati concernenti l'anomalia e alla compilazione della Scheda Evento (cfr. template A) allegato alla 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 Device 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, la DBAU, 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 e la funzione IT/Security si attiva per effettuare un raffinamento delle regole di rilevazione dei falsi positivi, comunicando via e-mail l'esito dell'analisi alla DBAU.

L'evento viene comunque inserito a cura della DBAU nel Registro dei Data Breach [tenuto a cura del DPO] (cfr. template C) in allegato alla presente procedura) nella apposita sezione dedicata agli "eventi falsi positivi"

C. ANALISI DI SECONDO LIVELLO – SCHEDA VIOLAZIONE DATI

Per l'analisi di secondo livello viene convocato il Data Breach Management Unit ("**DBMU**"), gruppo permanente a cui partecipano sinergicamente le seguenti strutture aziendali:

- IT/SECURITY;
- DPO (ove esistente)
- LEGAL (ove esistente);
- DIREZIONE SANITARIA
- EXECUTIVE PRIVACY
- RESPONSABILE DEL MARKETING
- RESPONSABILE/I DELLA/E AREA/E O PRODOTTI EVENTUALMENTE COMPROMESSI
- AMMINISTRATORE DELEGATO/DIRETTORE GENERALE (rappresentante del vertice aziendale)

In tutti i casi il DBMU analizza congiuntamente tutte le informazioni raccolte e redige una Scheda Violazione Dati (cfr. template B) allegato alla presente procedura) per le conseguenti valutazioni.

Il DBMU 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:

1. discriminazioni
2. furto o usurpazione d'identità
3. perdite finanziarie
4. pregiudizio alla reputazione
5. perdita di riservatezza dei dati personali protetti da segreto professionale
6. decifratura non autorizzata della pseudonimizzazione
7. danno economico o sociale significativo
8. privazione o limitazione di diritti o libertà
9. impedito controllo sui dati personali all'interessato
10. 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 DBMU 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 DBMU 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 DPO 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"** (cfr. par.4).

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 della Società 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 DBMU valuti che la violazione risulta presentare rischi classificati come ***"ALTI"*** nella Scheda Violazione Dati (cfr. template b) allegato alla presente procedura) 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 DBMU 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 DBMU.

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, se esistente, o di altro punto di contatto presso cui ottenere più informazioni;
d) le probabili conseguenze della Violazione dei Dati Personali;
e) la descrizione delle misure adottate o di cui si propone l'adozione da parte della Società 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.

La Società 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 (cfr. template C) allegato alla presente procedura), la DBAU documenta ogni singolo evento, sia esso, **FALSO**, **IRRILEVANTE** ovvero **RILEVANTE**; **in quest'ultimi due casi,** devono essere indicate nel registro:

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

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

Il Registro dei Data Breach è tenuto a cura del DPO sotto la responsabilità della società _____, 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 delle funzioni IT/Security, con eventuale supporto da parte di altre aree funzionali.

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

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 (solitamente il cliente per il quale offre servizi), senza ingiustificato ritardo secondo i tempi e i modi concordati nel contratto per il trattamento dei dati personali trasmesso da quest'ultimo (o in quelli concordati nel Contratto per il Trattamento dei Dati Personali allegato Linee guida sul Responsabile del Trattamento, se accettato dal Titolare come autonomina, o ancora nei modi previsti nella sezione VII.B che segue).

B. OBBLIGHI DI COMUNICAZIONE DI UN RESPONSABILE NEI CONFRONTI DELLA SOCIETÀ

Quando un terzo agisce in qualità di Responsabile (cfr. Linee guida sul Responsabile del Trattamento), in caso di Violazione dei Dati Personali, deve informare la Società (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@hsr.it
- [PEC] hsrsanraffaele@hsr.postecert.it

e successivamente collaborare con la Società per consentirgli 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.
[quanto segue è consigliabile ma ci aspettiamo che responsabili strutturati abbiano già procedure interne che rifletteranno gli obblighi di legge, e che quindi in pratica la procedura si concluderà qui. Ove invece il responsabile sia destrutturato e non abbia procedure per il caso di data breach, consigliamo/immaginiamo che sia possibile proseguire come segue]

Il Responsabile deve assistere la Società 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 Device 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 Società agli stessi indirizzi di cui sopra, al fine di consentirgli di inserire l'evento nella sezione "eventi falsi positivi" del Registro dei Data Breach (v. template 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 DPO Giorgio Presepio che nelle more devono essere costantemente tenuti allineati.

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

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

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] La Data breach assessment unit 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 Data breach management unit valuta il rischio secondo i seguenti livelli di rischio:

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

C. REGISTRO DEI DATA BREACH

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

D. 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 _____[5], alle ore_____;[6] di cui si è avuto conoscenza in

---

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.

[4] Inserire codice scheda evento

[5]

data_____alle ore_____;

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
- _____

A. Tra il __e il____
B. In un tempo non ancora determinato
C. È possibile che sia ancora in corso

[6] Indicare l'ora se nota, altrimenti indicare l'ora in cui si viene a conoscenza della violazione.

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, ove esistente/funzione legal funzione competente da identificarsi]_____ ai seguenti indirizzi:

Dati di contatto:

a) Nome e cognome del DPO, ove esistente
b) indirizzo di posta elettronica
c) indirizzo di posta PEC
d) indirizzo posta cartacea
e) numero telefonico dedicato
f) numero di fax dedicato
g) [ove esistente] *hot line* dedicata

Eventualmente *hot line dedicata [ove esistente]*

Data, Luogo _____

_____[il DPO, ove esistente/funzione legal/funzione competente da identificarsi]___

Distinti saluti