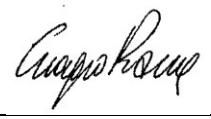
**Procedura Gestione dei Data Breach – rev. Settembre 2018**

# Procedura di Gestione delle violazioni dei dati personali (Data Breach Procedure Management)

# Pagina di controllo

| *Responsabile:* | |
|---|---|
| **AREA** | |
| **TIPOLOGIA** | Procedura |
| **ARGOMENTO** | Procedura di Gestione delle violazioni dei dati personali |
| **OBIETTIVO** | Assicurare una corretta gestione delle violazioni dei dati personali previste dalle normative sulle protezione dei dati personali |
| **DESTINATARI** | Tutto il personale dipendente, collaboratori e fornitori |
| **REDATTO DA** | Gruppo di lavoro della privacy |
| **COLLABORAZIONE DI** | DPO Enpaia |
| **APPROVATO (25/05/2018)** | |

| | |
|---|---|
| **EMANATO** |  |
| **RIFERIMENTI** | |
| **N. TOTALE PAGINE** | |

**STORIA DELLE MODIFICHE**

| NOME DEL FILE E CODIFICA | DATA | VERSIONE | RIFERIMENTO |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

INDICE

## 1. Introduzione

Il regolamento generale sulla protezione dei dati  UE 2016/679 (c.d. Gdpr) prescrive per il titolari del trattamento un nuovo adempimento generalizzato che consiste nella violazione dei dati personali (c.d. data breach), in precedenza e in base alla normativa italiana tale adempimento era infatti limitato solo ad alcuni specifici settori e contesti.

In tale contesto la Fondazione Enpaia in qualità di titolare del trattamento dei dati personali ritiene necessario di dotarsi di una procedura interna per la corretta gestione delle violazione dei dati personali.

In base al considerando 85 del Gdpr, una violazione dei dati personali (c.d. data breach) potrebbe, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali e immateriali alle persone fisiche.

A seguito di un violazione di dati personali possono derivare pregiudizi di varia natura dalla perdita di controllo dei dati personali alla limitazione diritti degli interessati compreso il furto o usurpazione di identità, pregiudizio alla propria reputazione e perdita di riservatezza, ma più in generale qualsiasi danno economico o sociale anche significativo agli interessati.

Al fine prevenire o mitigare tali pregiudizi, il titolare del trattamento ho l'obbligo, senza ingiustificato ritardo e ove possibile entro le 72 ore da quando ne è venuta a conoscenza, di notificare la violazione occorsa all'Autorità di Controllo competente. Il titolare viene ritenuto esente da tale obbligo qualora ritenga sotto la propria responsabilità che la violazione dei dati personali presenti un rischio improbabile in termini di pregiudizio per i diritti e le libertà delle persone fisiche.

## 2. Scopo

La presente procedura ha lo scopo di indicare le corrette modalità operative adottate da parte del titolare del trattamento dei dati personali, nel rispetto dei principi previsti dalle disposizioni del Regolamento UE 2016/679, per la gestione delle violazione dei dati personali ed in particolare:

- assicurare la migliore tutela per i diritti e libertà degli interessati;

- garantire una effettiva conformità rispetto al quadro normativo applicabile in materia di protezione dei dati personali;

- salvaguardare il proprio patrimonio informativo aziendale.

## 3. Ambito applicativo

Le politiche descritte nel presente documento si applicano a tutte a tutti i dipendenti e collaboratori della società i quali durante lo svolgimento delle loro attività possono venire a conoscenza di una violazione dei dati personali. Le presenti politiche si applicano anche ai fornitori nella misura in cui sono da considerarsi responsabile del trattamento ai sensi dell'articolo 28 del Gdpr e compatibilmente con procedure adottate e applicate dagli stessi.

In tal contesto è fatto obbligo loro di segnalare la violazione secondo le modalità indicate nelle presente procedura.

## 4. Ruoli e responsabilità

I responsabili della elaborazione, diffusione, del recepimento e dell'applicazione del presente documento sono:

- per l'elaborazione e la diffusione: tutti i compenti del Gruppo di Lavoro Privacy;
- per il recepimento e l'applicazione: il Componente del Gruppo di lavoro privacy delegato per la gestione della violazione dei dati (si rinvia al par. 7 per maggiori dettagli).

## 5. Definizioni, Termini e Acronimi

**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 (art. 4, punto 1).
**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, punto 2).
Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6).

**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, punto 7).
**Data Protection Officer (DPO):** la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).
**Gdpr:** Regolamento Generale per la protezione dei dati personali.
**Componente del Gruppo di lavoro Privacy delegato per la violazione dei dati ( articolo 29 del Regolamento UE 2016/679)**
: la persona fisica che, secondo l'organizzazione aziendale, ricopre un ruolo gestionale e di responsabilità all'interno di … che determina specifiche modalità organizzative rispetto ad uno o più trattamenti.
**Autorizzato al trattamento**: la persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (art. 4, punto 10).
**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, punto 8).
**Violazione dei dati personali** (c.d. Data breach):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 (art. 4, punto 12)
**CDVD**: Componente del Gruppo di lavoro privacy delegato per la gestione della violazione dei dati che coordina e supervisiona la corretta applicazione della procedura di gestione delle violazioni dei dati personal**i**

## 6. Documenti e normative di riferimento

Regolamento UE 679/2016, considerando n. 85, 86, 87, 88 artt. 33 e 34 del Gdpr

Decreto legislativo 196/2003 come modificato dal decreto legislativo del 10 agosto 2018, n. 101

Linee Guida "on Personal data breach notification under Regulation 2016/679 – WP article 29 (Adottate il 3 Ottobre 2017 – Revisionate il 6 Febbraio 2018)

Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali, Garante per la protezione dei dati personali (ed. aggiornata –Febbraio 2018)

## 7. Gestione del data breach da parte dei soggetti autorizzati al trattamento e notifica al Garante della protezione dei dati personali.

Ogni soggetto autorizzato al trattamento dei dati personali ai sensi dell'articolo 29 del GDPR e dell'art. 2 quaterdecies del d.lgs. 196/2003 (come modificato dal d.lgs. 10 agosto 2018, n. 101), qualora venga a conoscenza di un potenziale caso di una violazione dei dati personali, è tenuto ad avvisare tempestivamente il Componente del Gruppo di lavoro privacy delegato per la gestione della violazione dei dati che coordina e supervisiona la corretta applicazione della procedura di gestione delle violazioni dei dati personali (in seguito indicato anche con l'acronimo CDVD), tale figura coordina le attività di comunicazione al Garante e al DPO utilizzando il modulo allegato (All. 1)

Il CDVD formalmente incarico che riceve una segnalazione su un potenziale violazione dei dati personali è tenuto

A) La segnalazione viene inoltrata al Gruppo di lavoro privacy e viene immediatamente informato il DPO;
B) Si avviano gli accertamenti dovuti per comprendere il contesto del trattamento, la natura dei dati personali coinvolti e qualunque informazione utile per una completa valutazione dell'episodio;
C) Conclusi gli accertamenti e comunque non appena vengano individuati elementi chiari per la valutazione dell'episodio, si procederà a seconda dei casi a:

C.1) chiudere l'accertamento senza annotazione nel registro delle notificazioni qualora sia esclusa in modo chiaro una violazione dei dati personali (Vedi tabelle: 1. Modulo di accertamento e ispezione interna e 2. Modulo di valutazione del Rischio inerente il trattamento dei dati personali);

C.2) annotare la violazione dei dati personali nel Registro, senza effettuare alcuna notificazione qualora vi sia un rischio improbabile per i diritti e le libertà degli interessati;

C.3) annotare la violazione dei dati personali nel Registro ed effettuare la notificazione all'Autorità di Controllo nonché la comunicazioni agli interessati.

Nei casi indicati ai punti C.2 e C.3 è fatto obbligo al CDVD e al Gruppo di Lavoro Privacy coinvolgere immediatamente i vertici organizzativi del Titolare del trattamento anche al fine di valutare il coinvolgimento delle altre professionalità necessarie per l' analisi dell'accaduto.

Il CDVD e il Gruppo di Lavoro Privacy sono tenuti a consultare la Tabella di valutazione del rischio della violazione di dati personali, allegata alla presente procedura per decidere, sulla scorta delle determinazioni raggiunte, se effettuare l'eventuale comunicazione all'Autorità Garante.

Tale comunicazione, che sarà sottoscritta dal legale rappresentante del titolare del titolare del trattamento, deve essere inviata senza ingiustificato ritardo e, ove possibile, entro 72 ore; tale termine decorre dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza dal verificarsi della violazione.
Si specifica inoltre che nel caso in cui la comunicazione di cui al punto 3 sia effettuata successivamente al termine delle 72 ore, questa deve essere corredata delle ragioni del ritardo. E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione, anche a seguito di ulteriori indagini e attività di follow-up (c.d. notificazione in fasi)
Il CDVD coordina e verifica lo svolgimento della procedura di documentazione nell'apposito registro dell'episodio di violazione e che venga riportata anche la scelta e le motivazioni relative alle decisioni sulla necessità di notificare o meno l'evento.

## 8. Gestione data breach da parte dei Responsabili ex articolo 28 e notifica al Garante per la protezione dei dati

Qualora il trattamento di dati è affidato da parte del titolare del trattamento ad un soggetto terzo denominato Responsabile, così come disciplinato dall'articolo 28 del Regolamento sulla protezione dei dati personali (UE) 2016/679:

1) Ogni responsabile del trattamento, qualora venga a conoscenza di un potenziale data breach che riguardi dati di cui ….. è titolare, ne dà avviso senza ingiustificato ritardo al (soggetto) tramite il modulo allegato (All.2)
   Per "ingiustificato ritardo" si considera la notizia pervenuta a ….. al più tardi entro 12 ore dalla presa di conoscenza iniziale da parte del responsabile
2) Il Responsabile del trattamento deve garantire il reperimento delle informazioni su richiesta di ….. affinchè quest'ultima possa gestire il data breach
3) Ad ogni responsabile del trattamento deve essere comunicato (il soggetto) al quale effettuare la predetta segnalazione (indicare l'indirizzo mail;

4) Il soggetto effettua una valutazione dell'evento avvalendosi, se necessario, di eventuali altre professionalità necessarie per la corretta analisi della situazione. Il soggetto può avvalersi del DPO per eventuali funzioni consulenziali.
Ai fini di una corretta classificazione dell'episodio il (soggetto) utilizzerà lo schema di scenario di data breach allegato al presente schema di procedura. Pertanto, sulla scorta delle determinazioni raggiunte, il soggetto predispone l'eventuale comunicazione all'Autorità Garante, a firma del titolare, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.
Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo. E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi)
La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del referente privacy.
Rimane salva la possibilità che sia il responsabile del trattamento ad effettuare una notifica per conto del titolare del trattamento, se il titolare del trattamento ha rilasciato specifica autorizzazione al responsabile, all'interno del suddetto contratto. Tale notifica deve essere fatta in conformità con gli articoli 33 e 34 del GDPR. La responsabilità legale della notifica rimane in capo al titolare del trattamento.

## 9. Comunicazione della violazione dei dati personali all'interessato

Nel caso in cui dal data breach possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione. Il soggetto predispone l'eventuale comunicazione all'interessato/agli interessati, a firma del titolare, da inviarsi nei tempi e nei modi che lo stesso, anche attraverso la funzione consulenziale del DPO, individuerà come più opportuna come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità per la protezione dei dati personali.

## 10. Descrizione di violazione dei dati personali

Per facilitare l'individuazione della violazione dei dati evidenzia di seguito le diverse tipologie come indicate dalle Linee Guida W29. Il Presente paragrafo descrive alcune possibile violazioni dei dati personali ed utile alla compilazione della Tabelle A e B indicate al paragrafo 10.

Tipi di Violazioni (Data Breach)
a- Violazione della disponibilità, in caso di perdita o distruzione dei dati personali a seguito di accesso non autorizzato ai dati personali
b- Violazione dell'integrità, in caso di alterazione non autorizzata o accidentale dei dati personali
c- Violazione della riservatezza, in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali.

| TIPO DI VIOLAZIONE (DATA-BREACH) | DEFINIZIONE | Esempi |
|---|---|---|
| **A)Perdita di disponibilità dei dati.** | Tale violazione comporta che non si può accedere ai dati personali, quando un incidente di sicurezza rende non accessibili i dati personali, anche solo per un certo periodo. Tale ipotesi è da | 1- furto o smarrimento di un dispositivo(Hard Disk) contenente dati personali.<br>2- copia unica di dati personali crittografata da ransomware, o comunque crittografata utilizzando una chiave di cifratura non più disponibile<br>3- cancellazione volontaria o accidentale di dati di cui se ne deve |

| | | |
|---|---|---|
| | considerare un DB, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e libertà degli interessati | assicurare la conservazione<br>4- impossibilità di ripristinare l'accesso ai dati, ad esempio da un backup.<br>5- interruzione significativa del normale servizio anche in caso di interruzione di corrente o attacco denial of service, tale da rendere i dati personali non disponibili.<br>6- annullamento di attività che presuppongono un trattamento di dati personali a causa di un disservizio tecnico, per cui le persone potrebbero subire un serio danneggiamento.<br>7- perdita, anche solo temporanea, di disponibilità ( ad esempio nel caso in cui i dati possono essere successivamente ripristinati dal backup) causata da un'infezione dei sistemi informatici, ransomware. In tal caso, comunque, si è verificata un'intrusione nella rete del Titolare, con possibile DB.<br>8- pirata informatico contatta l'azienda dopo aver hackerato del sistema informatico per chiedere un riscatto.<br>9- distruzione o perdita di una copia o un backup di dati personali detenuti dai soggetti autorizzati a trattarli, ma i dati sono ancora detenuti dall'azienda.<br>10- Perdita di documenti contenenti categorie particolari di dati personali |
| **B)Violazione dell'integrità.** | Tale violazione comporta alterazione non autorizzata o accidentale dei dati personali | 1. Il Titolare rileva che c'è stata una possibile intrusione nella sua rete, che potrebbe aver compromesso l'integrità dei dati.<br>2. Modifica di dati personali o categoria di dati personali contenuti in documenti. |

| | | |
|---|---|---|
| **C)Violazione della riservatezza.** | Tale violazione riguarda la divulgazione o accesso non autorizzato o accidentale di dati personali | 1- di perdita di una chiave USB con dati personali non crittografati, di cui terzi potrebbero essere venuti in possesso<br>2 segnalazione, anche da parte di un terzo, di episodio nel quale un soggetto non autorizzato accidentalmente ricevuto dati personali relativi a soggetti interessati per trattamenti riferibili dal titolare.<br>3- in cui un terzo contatti l'azienda dopo aver hackerato il suo sistema per chiedere un riscatto.<br>4- in cui un terzo o un soggetto autorizzato a trattare i dati informa l'azienda di aver ricevuto dai suoi indirizzi mail una comunicazione non destinata a lui, contenente dati personali.<br>5. violazione della riservatezza e/o accesso non autorizzato a documenti contenenti categorie particolari di dati personali |

## 11. Registro delle violazioni

Il CDVD coordina e supervisiona l'aggiornamento del registro delle violazioni, ai sensi dell'art. 33,comma 5 del GDPR, verificando che siano state annotate tutte le informazione utili e necessarie per la gestione della possibile violazione dei dati personali (MOD 3).

## Tabelle per accertamenti e ispezioni preliminari

In questo paragrafo si riportano le tabelle relative alle informazioni minime che devono essere acquisite per l'accertamento o l'ispezione preliminare in caso si sospetti che sia avvenuta una violazione di dati personali (Tabella A), mentre l'altra tabella contiene una check list

per una valutazione ai fini del rischio inerente il trattamento dei dati personali in termini di pregiudizio sui diritti e le libertà degli interessati.

TABELLA 1 ACCERTAMENTI E ISPEZIONI PRELIMINARI IN CASO DI VIOLAZIONE DEI DATI PERSONALI

| Descrizione della sospetta violazione dei dati personali | Note a cura del Gruppo di Lavoro Privacy |
|---|---|
| Data e ora della scoperta delle sospetta violazione | |
| Data dell'incidente (se differente dalla scoperta) | |
| Luogo e contesto della violazione (specificare ogni elemento utile se relativo ad un documento oppure dispositivo elettronico, portatile, tablet, ecc., ecc.) | |
| Nome e dati di contatto della persona che ha effettuato la segnalazione della sospetta violazione (email, cellulare ed email), in caso di segnalazione di persona esterna riportare dati di contatti e nome del referente e ragione sociale se disponibili | |
| Descrizione dettagliata del contesto della violazione: supporto contenenti i dati personali sia cartaceo che elettronico | |

| | |
|---|---|
| | |
| Categoria di dati personali coinvolti nella sospetta violazione e numero approssimativo di interessati | |
| Descrizione delle eventuali azioni intraprese sin dal momento della scoperta | |
| Riportare osservazioni da parte del componente o dei componenti del Gruppo di Lavoro Privacy sulla sospetta violazione dei dati personali, laddove applicabile, specificando i motivi per l'eventuale esclusione della predetta violazione o la notificazione all'Autorità di Controllo e la comunicazione agli interessati | |
| Le indicazioni del componente o dei componenti del Gruppo di Lavoro Privacy devono contenere almeno una valutazione sommaria in ordine all'interpello del Data Protection Officer (DPO/RPD), qualora si escluso l'interpello del DPO/RPD tale esclusione deve essere motivata dal Componente delegato al coordinamento e alla supervisione del Gruppo di Lavoro Privacy (CDVD) | |
| Qualora non vi sia certezza in ordine all'esclusione della violazione dei dati personali occorre procedere alla valutazione del rischio inerente al | |

| | |
|---|---|
| trattamento secondo la tabella 2 | |
| In caso si proceda ad una valutazione ulteriore, a questo punto è obbligatorio coinvolgere immediatamente il DPO/RPD, se non si è ritenuto opportuno coinvolgerlo prima | |
| | |
| | |

TABELLA 2 - Check list per una valutazione ai fini del rischio inerente il trattamento dei dati personali

| Valutazione della presenza del rischio elevato per i diritti e libertà | Note a cura del Gruppo di Lavoro Privacy e del Data Protection Officer |
|---|---|
| Riportare informazioni aggiuntive, se disponibili, in ordine al supporto cartaceo o elettronico contenenti i dati personali (computer, tablet, documento cartaceo, ecc., ecc.) | |
| Descrivere la possibile esposizione al rischio dei dati personali (riservatezza, modifica parziale o totale degli stessi, disponibilità parziale o totale), anche con riferimento alla tabella indicata al paragrafo 8 del presente documento. | |

| | |
|---|---|
| Descrizione dettagliata delle possibili conseguenze negative relative ai dati personali coinvolti, specificare dal seguente elenco quali possono anche solo potenzialmente realizzarsi:<br><br>- un danno fisico, materiale o immateriale;<br>- se il trattamento può comportare 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;<br>- o qualsiasi altro danno economico o sociale significativo;<br>- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;<br>- se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;<br>- in caso di 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; | |

| | |
|---|---|
| - se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;<br>- se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati. | |
| Riportare una descrizione delle misure tecniche e organizzative applicate alla violazione dei dati personali occorsa (p.e. tecniche di cifratura, pseudonimizzazione, altra misura rilevante) | |
| Indicare se il Titolare ha adottato le misure atte scongiurare il sopraggiungere del rischio elevato per i diritti e libertà degli interessati | |
| Indicare se si è proceduto alla notificazione all'Autorità di controllo con descrizione della data e dei riferimento della notificazione | |
| Indicare se si è proceduto alla comunicazione agli interessati con descrizione delle specifiche modalità di comunicazione | |
| Documentare la violazione dei dati personali, riportando tutte le informazioni utili e come da modello di registro delle violazioni allegato | |
| | |

All 1)

## SEGNALAZIONE DI DATA BREACH

AL……

□ Il CDVD □ Autorizzato □ Amministratore di Sistema

Nome _____ Cognome_____

Struttura/Reparto_____ Indirizzo mail/altri dati di contatto_____

Segnala che:

Il /G/M/A/_____ alle ore _____

Si è verificata una violazione dei dati personali o (Data - Breach) che rientra in una delle seguenti tipologie (barrare la voce che interessa):

□ a- Violazione della disponibilità, in caso di perdita o distruzione dei dati personali a seguito di accesso non autorizzato ai dati personali

□ b- Violazione dell'integrità, in caso di alterazione non autorizzata o accidentale dei dati personali

□ c- Violazione della riservatezza, in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali

Descrizione della natura dei dati personali presumibilmente coinvolti e una descrizione dell'episodio

_____

_____

Data Firma

All.)2

SEGNALAZIONE DI DATA BREACH

AL……

Responsabile del Trattamento: _____

Nome _____ Cognome_____ (rappresentante legale)

Indirizzo mail_____

Segnala che: il /GG/MM/AAAA/_____ alle ore _____

si è verificato una violazione dei dati personali o (Data - Breach) che rientra in una delle seguenti tipologie (barrare la voce che interessa):

□ a- Violazione della disponibilità, in caso di perdita o distruzione dei dati personali a seguito di accesso non autorizzato ai dati personali

□ b- Violazione dell'integrità, in caso di alterazione non autorizzata o accidentale dei dati personali

□ c- Violazione della riservatezza, in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali

Descrizione della natura dei dati personali presumibilmente coinvolti e una descrizione dell'episodio

_____

_____

Data Firma

All.3)

## Registro delle violazioni di dati personali o data breach ai sensi dell'articolo 33 comma 5 del Gdpr

| Data violazione | Natura della violazione e categorie di dati personali coinvolti | Servizio/UO coinvolto | Categorie degli interessati coinvolti | Numero Interessati coinvolti | Categorie e numero approssimativo di registrazioni | Probabili conseguenze della violazione | Misure adottate o di cui si propone l'adozione per mitigare i rischi e possibili effetti negativi | Notifica Autorità Garante per la Protezione dei dati (data e ora, rifermento per reperire la notifica) | Comunicazione interessati (data e ora, modalità di comunicazione) | Comunicazione all'Autorità Garante dei Dati di contatto del DPO e/o di altro punto di contatto più informato (indicare se e quali dati sono stati comunicati) |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |

# DISPOSIZIONI OPERATIVE DI PREVENZIONE DEL DATA BREACH

Ai dipendenti e collaboratori

Spettabile dipendente o collaboratore, la Fondazione ENPAIA, in qualità di Titolare del trattamento, ha adottato una politica specifica volta alla prevenzione e contenimento degli incidenti di sicurezza e più specificatamente alle eventuali violazioni di dati personali.

Al riguardo si dispone che:

Qualora il dipendente o il collaboratore abbia notizia di un furto o smarrimento o di documentazione che riporta dati personali e sensibili o di dispositivo di memoria, e quindi della eventuale possibilità che terzi possano aver avuto accesso non autorizzato a tali dati è obbligatoria la immediata comunicazione/segnalazione all'índirizzo mail databreach@enpaia.it impiegando i moduli descritti nella presente politica di sicurezza.

Analoga attività deve essere assicurata in caso di:

- eventuali comunicazioni di dati, anche via mail, a soggetti diversi dagli autorizzati al trattamento dei dati, di specifico riferimento o nel caso in cui i dati personali non siano più disponibili a causa di distruzione, cancellazione o di altri problemi di natura anche automatizzata, come ad esempio un virus;

-ricezione, anche tramite l´Ufficio relazioni con il pubblico, di notizia di possibile Data Breach, ad esempio nel caso in cui un terzo informi di aver ricevuto dalla struttura sanitaria una comunicazione non destinata a lui contenente dati personali.