Ordine
dei tecnici sanitari di radiologia medica
e delle professioni sanitarie tecniche,
della riabilitazione e della prevenzione
di Bologna

PROCEDURA OPERATIVA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI AI SENSI DEL REGOLAMENTO EUROPEO 679/2016

"DATA BREACH"

Approvata dal Consiglio Direttivo dell'Ordine dei TSRM e PSTRP di Bologna con delibera n. 60/2022 in data 05/05/2022

Sommario

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org

PREMESSA

L'art. 33 del Regolamento generale sulla protezione dei dati 679/2016 G.D.P.R. ha introdotto l'obbligo in capo al Titolare del trattamento di notifica all'Autorità di controllo – Autorità Garante per la protezione dei dati personali (d'ora in poi per brevità Autorità Garante) - delle violazioni dei dati personali (c.d. data breach).

Una violazione dei dati personali (c.d. data breach) se non affrontata in modo adeguato e tempestivo può provocare danni fisici, materiali o immateriali alle persone fisiche: quali la perdita del controllo dei dati personali che li riguardano o la limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Per prevenire o mitigare tali pregiudizi, **il Titolare del trattamento** deve notificare la violazione, **senza ingiustificato ritardo e, ove possibile entro 72 ore da quando ne è venuto a conoscenza** all' Autorità Garante.

L'obbligo di comunicazione viene meno solo qualora il Titolare ritenga che la violazione dei dati personali presenti un rischio improbabile in termini di pregiudizio per i diritti e le libertà delle persone fisiche.

Nel caso di rischio elevato, oltre alla notifica all'Autorità Garante, **il Titolare è tenuto a dare comunicazione della violazione anche all'interessato ai sensi dell'art. 34 del G.D.P.R.**

Qualora la notifica non sia effettuata entro 72 ore, essa dovrà essere corredata dei motivi del ritardo.

A fronte del mancato rispetto dell'obbligo di notifica l'Autorità Garante può:

- applicare misure correttive previste dall'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati);
- oppure in aggiunta o in luogo delle misure correttive di cui all'art. 58 GDPR irrogare sanzioni amministrative pecuniarie ai sensi dell'art. 83 GDPR (fino a 10.000,000 Euro e per le imprese fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore).

SCOPO DELLA PROCEDURA

L'Ordine dei Tecnici Sanitari di Radiologia Medica e delle Professioni Sanitarie Tecniche, della Riabilitazione e della Prevenzione della Provincia di Bologna (d'ora in poi per brevità Ordine dei TSRM e PSTRP di Bologna), nella sua qualità Titolare del trattamento dei dati personali, ha predisposto la presente procedura interna per una corretta e rapida gestione delle violazioni dei dati personali al fine di:

- assicurare il rispetto delle prescrizioni del G.D.P.R.;
- garantire la migliore tutela dei diritti e libertà dei soggetti interessati (quali iscritti, componenti del Consiglio Direttivo, componenti Commissioni d'albo, consulenti, fornitori, addetti alla segreteria)

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org

- salvaguardare il proprio patrimonio informativo istituzionale.

Di seguito sono individuate le modalità operative di gestione delle violazioni dei dati personali (individuazione della violazione; - ruoli e compiti all'interno dell'Ordine dei TSRM e PSTRP di Bologna nella gestione del data breach; - accertamenti da effettuare, modalità di notifica etc.).

NORMATIVA E DOCUMENTI DI RIFERIMENTO

La presente procedura è stata redatta sulla base della seguente normativa e documentazione:

- *Regolamento UE 679/2016, considerando n. 85, 86, 87, 88 artt. 33, 34;*
- *Decreto legislativo 196/2003, modificato dal decreto legislativo del 10 agosto 2018, n. 101*
- *Linee Guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE 2016/679 elaborate dal Gruppo di lavoro articolo 29 per la protezione dei dati personali, adottate il 3 ottobre 2017- versione emendata e adottata in data 6 febbraio 2018.*

In particolare si riportano **integralmente gli artt. 33 e 34 del G.D.P.R**.

Art. 33 del GDPR "*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.
   e) 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.

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org

f) 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 del GDPR *"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.

DEFINIZIONI GENERALI

- «***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 GDPR);
- "***categorie particolari di dati personali***": dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 G.D.P.R.);

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org

- "***Dati relativi a condanne penali e reati***": dati personali relativi a condanne penali e a reati o connessi a misure di sicurezza (art. 10 G.D.P.R.);
- *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 GDPR);
- «***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 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 (art. 4, punto 8 GDPR);
- "***autorizzato al trattamento***": persona fisica, espressamente designata che opera sotto l'autorità del Titolare del trattamento (art. 29 GDPR e art. 2-quaterdecies D.lgs. n. 196/2003, modificato dal D.Lgs. 10 agosto 2018, n. 101,
- **«*violazione dei dati personali*»:** 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 GDPR);
- **«*autorità di controllo»:*** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 (art. 4, punto 21 GDPR- art. 2 bis D.lgs. n. 196/2003, modificato dal D.Lgs. 10 agosto 2018, n. 101);

AMBITO DI APPLICAZIONE DELLA PROCEDURA

La presente procedura è rivolta:

- **ai soggetti autorizzati al trattamento** che durante lo svolgimento dei propri compiti possono venire a conoscenza di una violazione dei dati personali;
- **ai soggetti esterni all'Ente** (quali ad. esempio Responsabili del trattamento, soggetti interessati) che possono venire a conoscenza di una violazione dei dati personali

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org

GESTIONE DATA BREACH

I FASE: SEGNALAZIONE

Ciascun **soggetto autorizzato al trattamento** che venga a conoscenza di una violazione dei dati personali è tenuto:

- ad avvertire **immediatamente** il **Referente privacy** contattandolo telefonicamente;

- successivamente a **compilare, entro e non oltre 1 ora dalla conoscenza della violazione, il modello 1** messo a diposizione dal Titolare da inviare all'indirizzo di posta elettronica bologna@tsrm.org, alla c.a del Referente privacy, indicando con oggetto: "*segnalazione data breach".*

- Ciascun **soggetto esterno all'Ente** che venga a conoscenza di una violazione dei dati personali può segnalare la violazione scrivendo all'indirizzo di posta elettronica bologna@tsrm.org, alla c.a del Referente privacy, indicando come oggetto: "*segnalazione data breach".*

II FASE: GESTIONE DELLA SEGNALAZIONE DA PARTE DEL REFERENTE PRIVACY

Il Referente privacy, delegato dal Titolare del trattamento a coadiuvarlo nella gestione della procedura delle violazioni dei dati personali, **riferisce immediatamente al Presidente dell'Ordine e ai Componenti del Consiglio Direttivo sulla segnalazione ricevuta, informando altresì il DPO della presunta violazione**, quindi:

1) effettua gli accertamenti necessari per comprendere il contesto del trattamento, la natura dei dati personali coinvolti e qualunque informazione utile per una completa valutazione dell'episodio, anche avvalendosi a seconda della violazione di professionisti esterni, quali consulenti informatici, legali e/o consulenti esperti in materia di privacy al fine di mitigare e attenuare i rischi derivanti dalla possibile violazione, coadiuvato dal D.P.O,

2) informa il Responsabile del trattamento dei dati allorquando la violazione coinvolga dati trattati da un Responsabile del trattamento, ciò al fine di far avviare tutte le verifiche necessarie;

3) documenta l'esito preliminare dell'indagine utilizzando **il modello 2**;

4) conclusi gli accertamenti, **nelle successive 12 ore dalla scoperta della presunta violazione,** trasmette la documentazione al Presidente e ai Componenti del Consiglio Direttivo per la valutazione.

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org

III FASE: VALUTAZIONI DEL TITOLARE E ATTIVITÀ CONSEGUENTI

Il Consiglio Direttivo, immediatamente convocato, anche in modalità telematica, valutati gli elementi a disposizione, con l'ausilio del DPO e di professionisti informatici (ove necessario il loro coinvolgimento tenuto conto della tipologia di violazione):

- chiude l'accertamento senza annotazione nel registro delle notificazioni qualora sia palese che la violazione non riguarda dati personali;
- in caso di accertata violazione dei dati personali, potrà:

a) dispone l'annotazione della violazione nel Registro a cura del Referente privacy senza effettuare alcuna notificazione qualora sia improbabile che essa presenti un rischio per i diritti e le libertà degli interessati;

b) in caso di rischio ai diritti e alle libertà degli interessati, dispone l'annotazione della violazione nel Registro a cura del Referente privacy ed effettua la notificazione all'Autorità Garante. Qualora il rischio ai diritti e alle libertà degli interessati sia elevato oltre all'annotazione nel Registro, effettua la comunicazione agli interessati sussistendo i presupposti di cui dall'art. 34 del G.D.P.R.

VIOLAZIONE DEI DATI PERSONALI

Affinché tutti i soggetti coinvolti nella procedura di data breach possano svolgere i compiti di rispettiva competenza è necessario chiarire che cosa si intende per violazione dei dati personali.

Ai sensi dell'art. 4, punto 12 del GDPR per violazione dei dati personali si intende: 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.

La violazione di dati personali è quindi un **particolare tipo di incidente di sicurezza.**

È importante chiarire che non tutti gli incidenti di sicurezza sono necessariamente violazioni di dati personali.

Le violazioni di dati personali si distinguono in:

1. "*violazione di riservatezza*", in caso di divulgazione dei dati personali o acceso agli stessi non autorizzati o accidentali;
2. "*violazione di integrità"*, in caso di modifica non autorizzata o occidentale dei dati personali;
3. "*violazione di disponibilità*", in caso di perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org

Di seguito si riporta una tabella in cui sono indicate in via meramente esemplificativa possibili violazioni di dati personali:

TIPO DI VIOLAZIONE DATA BREACH	DEFINIZIONE	ESEMPI
1. VIOLAZIONE DELLA RISERVATEZZA	In caso di divulgazione o accesso non autorizzato o accidentale di dati personali	1-perdita di una chiave USB con dati personali non crittografati di cui terzi potrebbero essere venuti in possesso 2- segnalazione, anche da parte di un terzo, di un episodio nel quale un soggetto non autorizzato accidentalmente ha ricevuto dati personali
2. VIOLAZIONE DELL'INTEGRITÀ	in caso di modifica non autorizzata o occidentale 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. 2- Modifica di dati personali o categorie di dati personali contenuti in documenti.
a) Perdita di disponibilità dei dati	in caso di perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.	1- furto o smarrimento di un dispositivo (Hard Disk) contenente dati personali. 2 -furto computer dall'ufficio 3- copia unica di dati personali crittografata da ransomware, o comunque crittografata utilizzando una chiave di cifratura non più disponibile 3cancellazione volontaria o accidentale di dati di cui se ne deve assicurare la conservazione 4- impossibilità di ripristinare l'accesso ai dati, ad esempio da un backup. 5- interruzione significativa del normale servizio anche in caso di interruzione di corrente o attacco da blocco di servizio, tale da rendere i dati personali non disponibili.

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org

		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. 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. 8- pirata informatico contatta l'Ordine dopo aver hackerato il sistema informatico per chiedere un riscatto. 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. 10- Perdita di documenti contenenti categorie particolari di dati personali

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE

Una volta che il Titolare ha appurato che è avvenuta una violazione dei dati personali sarà necessario capire se da essa possono derivare rischi ai diritti e alle libertà delle persone onde verificare l'obbligatorietà della notifica al Garante ed eventualmente ai soggetti interessati.

Il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche:

1. discriminazioni
2. furto o usurpazione d'identità
3. perdite finanziarie
4. pregiudizio alla reputazione

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org

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.

In caso di:

- Rischio assente: la notifica al Garante non è obbligatoria. Tale ipotesi si verifica ad esempio quando i dati personali, oggetto della violazione, sono dati pubblici.
- Rischio presente: è necessaria la notifica al Garante.
- Rischio elevato: è necessaria la notifica al Garante e la comunicazione anche agli interessati. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali (ad. esempio dati vaccinali);
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati bancari);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni.

NOTIFICA AL GARANTE: TEMPI, CONTENUTO

Il Titolare in caso di violazione dei dati personali provvede senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza** (cioè quando abbia un ragionevole grado di certezza del verificarsi della violazione) a notificare la violazione all'Autorità Garante.

Se la comunicazione è effettuata successivamente al termine delle 72 ore, questa deve essere corredata delle ragioni del ritardo.

È 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).

La notifica va trasmessa al Garante per la protezione dei dati personali con modalità telematica accedendo alla piattaforma dedicata https://servizi.gpdp.it/databreach/s/ e seguendo le modalità ivi indicate.

La notifica dovrà contenere i seguenti elementi:

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org

a) descrizione della 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) nome e i dati di contatto del Titolare o di altra persona presso cui ottenere più informazioni;
c) descrizione delle probabili conseguenze della violazione dei dati personali;
d) descrizione delle 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

Il Referente privacy sulla base della decisione assunta dal Consiglio Direttivo, coadiuvato dal DPO e dalla società informatica e/o consulente informatico eventualmente incaricato, curerà la compilazione della comunicazione seguendo le istruzioni contenute sul sito istituzionale del Garante della Privacy https://servizi.gpdp.it/databreach/s/. Si allega fac simile per le comunicazioni (**modello 3**)

COMUNICAZIONE AGLI INTERESSATI

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 Referente privacy, coadiuvato dal DPO, predispone una comunicazione con un linguaggio semplice e chiaro da inviare all'interessato/agli interessati e da lui sottoscritta.

La comunicazione deve contenere:

a) nome e i dati di contatto del Titolare o di altra persona presso cui ottenere più informazioni;
b) descrizione delle probabili conseguenze della violazione dei dati personali;
c) descrizione delle 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.

Non è richiesta la comunicazione all'interessato 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;

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org

c) la 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.

COMPITI DEI RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 GDPR

Ogni Responsabile del trattamento, qualora venga a conoscenza di un potenziale data breach che riguardi dati personali che tratta per conto del Titolare, informa il Titolare tempestivamente di essere venuto a conoscenza di una violazione, nei termini e con le modalità convenute nei contratti di nomina come Responsabile del trattamento ex art. 28 G.D.P.R.

Il Responsabile dovrà indicare:

- una descrizione della natura della violazione della sicurezza, comprendente il volume e la tipologia di dati personali, le categorie e il numero approssimativo di persone interessate;
- le conseguenze probabili della violazione della sicurezza;
- una descrizione delle misure adottate o proposte per far fronte alla violazione della sicurezza, ivi comprese, se del caso, le misure atte a mitigarne i possibili effetti negativi.

Il Responsabile del trattamento:

- fornisce assistenza al Titolare per far fronte alla violazione e alle sue conseguenze soprattutto in capo agli interessati coinvolti;
- intraprende tutte le azioni correttive necessarie e appropriate, a spese proprie, per prevenire il ripetersi di tale violazione della sicurezza dei dati personali.

Il Titolare del trattamento, ricevuta la comunicazione della violazione di sicurezza da parte del Responsabile del trattamento, effettua gli accertamenti ritenuti necessari al fine di valutare la sussistenza degli obblighi di cui agli artt. 33 e 34 del G.D.P.R. secondo quanto indicato nei precedenti paragrafi.

REGISTRO DELLE VIOLAZIONI DEI DATI PERSONALI

Al fine di documentare le violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, l'Ordine dei TSRM e PSTRP di Bologna ha predisposto il registro delle violazioni dei dati personali ai sensi dell'art. 33, comma 5, del GDPR.

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org

Il Referente privacy delegato ne curerà la compilazione in caso di eventuali data breach, inserendo tutte le informazioni utili e necessarie per la gestione della violazione dei dati personali.

CASISTICA LINEE GUIDA

Di seguito si riporta una tabella, tratta dalle *Linee Guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE 2016/679, elaborate dal Gruppo di lavoro articolo 29 per la protezione dei dati, adottate il 3 ottobre 2017, versione emendata e adottata in data 6 febbraio 2018,* contenente alcuni esempi di possibili violazioni di dati personali e di comportamenti da assumere. L'elencazione è meramente esemplificativa:

ESEMPIO	**NOTIFICA ALL'AUTORITA' GARANTE?**	**COMUNICAZIONE ALL'INTERESSATO?**	**NOTE/ RACCOMANDAZIONI**
Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No	No	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare del	no	no	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. Il titolare del trattamento deve conservare adeguate registrazioni in merito.

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org

trattamento e accedere alle proprie registrazioni.			
Un titolare del trattamento subisce un attacco tramite *ransomware* che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa evidente che l'unica funzionalità dal *ransomware* era la cifratura dei dati e che non vi erano altri *malware* presenti nel sistema.	Sì, effettuare la segnalazione all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	Sì, effettuare la segnalazione alle persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	Se fosse stato disponibile un backup e i dati avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'autorità di controllo fosse venuta a conoscenza dell'incidente con altri mezzi, avrebbe potuto prendere in considerazione lo svolgimento di un'indagine al fine di valutare il rispetto dei requisiti di sicurezza più ampi di cui all'articolo 32.
Una e-mail viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se è interessato un numero elevato di persone, se vengono rivelati dati sensibili o se altri fattori presentano rischi elevati (ad esempio, il	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato soltanto un numero limitato di indirizzi di posta elettronica.

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org

	messaggio di posta elettronica contiene le password iniziali).		

Casalecchio di Reno (Bo), 05/05/2022

Il Titolare del Trattamento dei dati personali

Il Consiglio Direttivo dell'Ordine TSRM-PSTRP di Bologna

In persona del Presidente Dott. Vincenzo Manigrasso

Indirizzo: Via G. Gaspari, 5/3 – 40033 Casalecchio di Reno (BO)
Tel. 051348892 – Fax 051348892
C.F. 80080390372 – Sito Internet: www.bolognatsrmpstrp.it
Posta elettronica ordinaria: bologna@tsrm.org PEC: bologna@pec.tsrm.org