# Procedura per la gestione delle violazioni dei dati personali (Data Breach)

(Art. 33 e 34 del Regolamento UE 2016/679)

**Indice**

## Premessa

La presente procedura di gestione delle violazioni dei dati personali, o "Data Breach", ha lo scopo di fornire le indicazioni operative in caso di violazione dei dati personali di cui l'Azienda Ospedaliero-Universitaria Policlinico "G. Rodolico – San Marco" è titolare del trattamento.

## 1. Scopo

Scopo della presente procedura è definire i compiti, le responsabilità e le modalità operative in caso di violazione dei dati personali trattati da o per conto dell'Azienda Ospedaliero-Universitaria Policlinico "G. Rodolico – San Marco".

Con la procedura il Titolare del trattamento dei dati personali recepisce e pone in atto quanto previsto dagli articoli 33 e 34 del Regolamento (UE) 2016/679, e nei vari provvedimenti emessi dal Garante per la tutela dei dati personali, applicabili al Servizio Sanitario Nazionale, tra cui il provvedimento n. 393 del 2 luglio 2015 "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche".

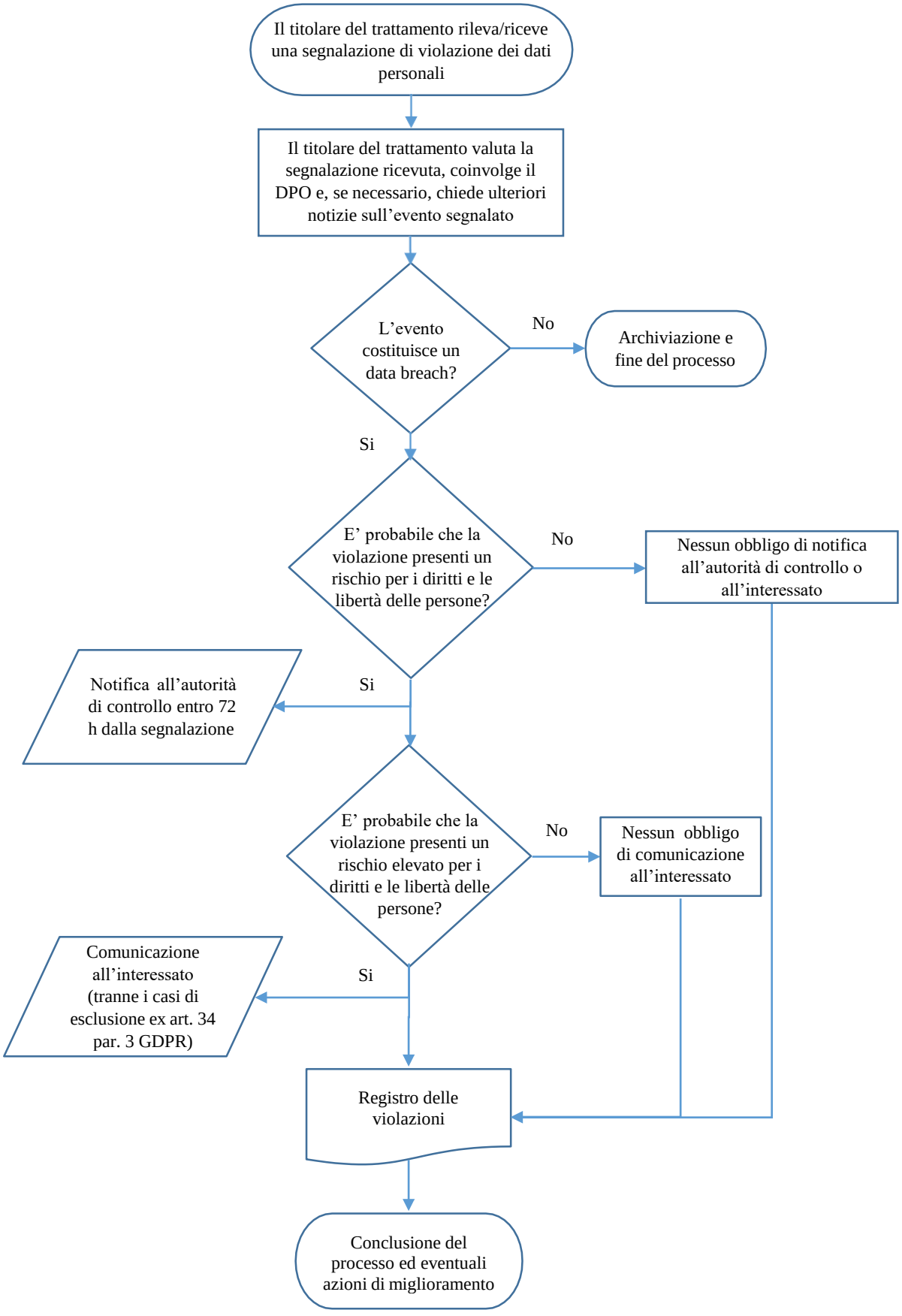
## 2. Campo di applicazione

La procedura si applica a tutti i dipendenti e collaboratori dell'Azienda Ospedaliero-Universitaria Policlinico "G. Rodolico – San Marco" individuati quali soggetti designati ed incaricati ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/2003, e pertanto autorizzati a trattare dati personali di cui l'Azienda Ospedaliero-Universitaria Policlinico "G. Rodolico – San Marco" è titolare.
La procedura è rivolta altresì a qualsiasi soggetto, persona fisica o giuridica, che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento effettua un trattamento di dati personali in qualità di Responsabile esterno del trattamento ex art. 28 GDPR.
Il rispetto della presente procedura è obbligatorio per tutti i soggetti sopra richiamati e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero l'applicazione di sanzioni nei confronti delle terze parti inadempienti, secondo le normative vigenti in materia.

## 3. Riferimenti normativi

- Decreto Legislativo n. 196/2003 e successive modifiche ed integrazioni (Codice privacy);
- Regolamento (UE) 2016/679 (GDPR, General Data Protection Regolation);
- Regolamento aziendale per la protezione dei dati personali;
- Provvedimento del Garante per la protezione dei dati personali n. 393 del 2 luglio 2015 "Misure disicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche";
- Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679 (wp250rev.01).

## 4. Diagramma di flusso



## 5. Definizione di violazione dei dati personali (data breach)

Si intende per 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 dal Titolare del trattamento.

Il Gruppo di lavoro Articolo 29 per la protezione dei dati personali ha identificato i seguenti tipi di data breach:

- "**violazione della riservatezza**": in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "**violazione dell'integrità**": in caso di modifica non autorizzata o accidentale dei dati personali;
- "**violazione della disponibilità**": in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Le violazioni di dati personali possono accadere per un ampio numero di situazioni che, a titolo esemplificativo, possono includere:

- perdita, furto o violazione di documentazione cartacea;
- perdita, furto o violazione di PC desktop, PC portatili, dispositivi di memoria (pen drive, hard disk, ecc.), devices o altre attrezzature contenenti dati personali di cui l'Azienda è titolare del trattamento;
- divulgazione di dati confidenziali a persone non autorizzate;
- accesso ai dati da parte di persona non autorizzata (ad esempio: accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- alterazione o distruzione di banche dati senza autorizzazione rilasciata dal titolare o responsabile;
- virus o altri attacchi al sistema informatico o alla rete aziendale che compromettono il funzionamento dei servizi aziendali;
- violazione di una casella di posta elettronica aziendale.
- invio di e-mail contenenti dati personali e/o particolari a destinatario errato.

## 6. Descrizione delle attività

### 6.1. Acquisizione di notizia di violazione

Qualunque soggetto autorizzato al trattamento dei dati personali di cui l'Azienda è titolare (soggetti designati, incaricati e Responsabili del trattamento), qualora si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente informare il superiore gerarchico per la segnalazione della violazione al Titolare del trattamento.
La segnalazione dovrà essere effettuata mediante la compilazione dell'Allegato A – Modulo di comunicazione di Data Breach - da trasmettere, nel più breve tempo possibile, al titolare del trattamento all'indirizzo mail privacy@policlinico.unict.it.
Parimenti, qualora la rilevazione avvenga a cura di un soggetto terzo esterno all'organizzazione (es. Responsabile del trattamento), questi informa il Titolare del trattamento senza ingiustificato ritardo, ai sensi dell'art. 33 comma 2 Regolamento (UE), con le medesime modalità di cui sopra.
In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenirne una reiterazione.

### 6.2. Identificazione dell'evento e sua valutazione

Il Titolare del trattamento, avuta notizia dell'avvenuto o potenziale data breach, avvia l'istruttoria per l'identificazione e l'analisi dell'evento, richiedendo eventualmente ulteriori notizie al personale della struttura che ha segnalato l'evento nonché copia dell'eventuale segnalazione agli Organi di Polizia.
Ai fini della valutazione dell'incidente occorso il Titolare del trattamento consulta il DPO e, nel caso di violazione dei sistemi informatici, acquisisce le necessarie notizie dal Direttore del CED o da un suo delegato in caso di assenza.
La valutazione prevede l'analisi delle informazioni relative all'evento, tra cui:
• la data di scoperta della violazione;
• Il soggetto che è venuto a conoscenza della violazione;
• la descrizione dell'evento (natura della violazione e dei dati coinvolti);
• le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
• la descrizione delle misure tecniche e organizzative analogiche e/o digitali adottate per attenuare i possibili effetti negativi della violazione.
La valutazione ha lo scopo di stabilire se l'evento costituisce o meno una violazione dei dati personali ai sensi di quanto previsto dagli art. 33 e 34 del GDPR.

### 6.3. Valutazione del rischio per i diritti e le libertà delle persone fisiche

Attraverso la compilazione della scheda di cui al modello allegato B il titolare del trattamento, sulla base delle valutazioni effettuate dal DPO, determina la gravità della violazione, ovvero la possibilità che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
Ai fini della gestione del Data Breach occorre considerare se:

- i dati siano stati in precedenza resi anonimi oppure pseudonimizzati;
- i dati siano stati oggetto di cifratura e se fosse garantita, al momento della violazione, la riservatezza della chiave di decifratura;
- i dati violati non siano riconducibili all'identità di persone fisiche;
- i dati siano già stati oggetto di pubblicazione.

Se si tratta di una violazione di riservatezza occorre pertanto verificare se le misure di sicurezza adottate (es.: cifratura dei dati) rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note). In caso di perdita di integrità o disponibilità dei dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati.
Qualora sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche e il titolare ritenga non opportuno procedere alla notifica della violazione, la procedura si conclude compilando il Registro delle violazioni con annotazione delle motivazioni e scelte operate. In tal caso le misure messe in atto sono risultate adeguate alla minaccia. Potranno eventualmente essere avviate misure di miglioramento per incrementare ulteriormente la protezione dei dati.
Qualora il Titolare del trattamento ed il DPO abbiano opinioni discordanti circa l'insussistenza del rischio per i diritti e le libertà degli interessati, la decisione sull'opportunità di notificare la violazione dei dati personali all'autorità di controllo ricadrà unicamente sul Titolare del trattamento e dovrà essere debitamente motivata.

### 6.4. Notifica all'autorità di controllo

Ai sensi dell'art. 33 del GDPR, la notifica del Data Breach all'Autorità di controllo è sempre obbligatoria, salvo i casi in cui sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Pertanto, rilevata l'esistenza di un rischio per i diritti e le libertà degli interessati e ritenuto doversi effettuare la notifica della violazione dei dati subita, secondo quanto prescritto dal Regolamento (UE) 2016/679, l'Azienda dovrà provvedervi, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza, utilizzando il format e le procedure previste dall'autorità di controllo.
Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, essa dovrà essere corredata dei motivi del ritardo.
Se non fosse possibile fornire tutte le informazioni contestualmente, queste ultime potranno essere inviate in fasi successive senza ulteriore ingiustificato ritardo, avendo cura di dare evidenza delle motivazioni per cui tali informazioni non sono disponibili.
In questo caso sarà cura del Titolare del trattamento raccogliere le informazioni mancanti e procedere, senza ritardo, alle integrazioni eventualmente necessarie avvalendosi della collaborazione delle strutture interessate che, a tal fine, dovranno prestare pronta, piena e fattiva disponibilità.
La mancata collaborazione del personale e strutture coinvolte assume rilevanza ai fini disciplinari e contrattuali.
Ai sensi dell'art. 33 del GDPR, la notifica all'autorità di controllo deve contenere almeno i seguenti contenuti:

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) indicazione del nome e dei dati di contatto del Data Protection Officer o di altro punto dicontatto 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.

La violazione sarà effettuata dal titolare del trattamento tramite PEC con indicazione del DPO come punto di contatto con l'Autorità di controllo.

### 6.5. Comunicazione all'interessato

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.
Ai sensi dell'art. 34 del GDPR, la comunicazione all'interessato dovrà descrivere, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali e deve contenere almeno le seguenti informazioni:

- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la 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, se del caso, per attenuarne i possibili effetti negativi;
- il nominativo e i dati di contatto del DPO.

Ai sensi dell'art. 34, paragrafo 3, non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto 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;

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.

## 7. Registro delle violazioni

L'Azienda documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. A tal riguardo l'Azienda predispone un registro interno delle violazioni e segnalazioni di violazione dei data breach e ciò indipendentemente dalle notifiche all'autorità di controllo.
Il Registro delle violazioni, di cui al modello allegato C, dovrà contenere le informazioni di seguito riportate:
(i) n. evento; (ii) data della violazione; (iii) data della segnalazione; (iv) nominativo del segnalante; (v) luogo della violazione; (vi) descrizione della violazione; (vii) dispositivo/applicativo oggetto di violazione; (viii) categorie di dati personali coinvolti; (ix) tipologia di violazione; (x) categorie e numero approssimativo di soggetti interessati dalla violazione; (xi) categorie e numero approssimativo di registrazioni dei dati; (xii) probabili conseguenze della violazione; (xiii) valutazione del rischio per i diritti e le libertà delle persone fisiche; (xiv) misure e provvedimenti adottati; (xv) se sia stata effettuata o meno notifica all'autorità di controllo; (xvi) se sia stata effettuata o meno la comunicazione agli interessati; (xvii) note e commenti.
Il Registro delle violazioni è tenuto in formato elettronico dal DPO e da questi continuamente aggiornato. Esso viene messo a disposizione del Garante per la protezione dei dati personali qualora l'Autorità chieda di accedervi.

## 8. Modulistica allegata alla procedura

Allegato A – Modello per la segnalazione di violazione dei dati personali

Allegato B – Scheda di valutazione della violazione dei dati personali

Allegato C – Modello di Registro delle violazioni dei dati personali

**Allegato A - Modello per la segnalazione di violazione dei dati personali**

## Segnalazione di violazione dei dati personali (Data breach)

Al Direttore Generale
Al Data Protection Officer
AOU Policlinico "G.Rodolico – San Marco"
mail: privacy@policlinico.unict.it

Il sottoscritto .....

Contatto telefonico ..... E mail .....

In qualità di ☐ soggetto designato/incaricato del trattamento presso l'U.O. di .....
☐ Responsabile esterno del trattamento

**Comunica la seguente violazione dei dati personali:**

**Data e ora della presunta violazione:** ...../...../..... Ore .....

**Descrizione della violazione:**

.....

.....

.....

.....

**Tipologia di violazione:**

☐ Perdita/furto/violazione di PC desktop ☐ Perdita/furto/violazione di PC portatile

☐ Perdita/furto di dispositivi di memoria ☐ Perdita/furto/violazione di documenti cartacei

☐ Virus o attacchi informatici ai sistemi aziendali ☐ Violazione di casella di posta elettronica aziendale

☐ altro .....

**Categorie di dati personali coinvolti nella violazione:**

☐ Dati comuni ☐ Dati particolari (relativi alla salute, dati genetici, dati biometrici)

Tipo di dati coinvolti .....

**Numero approssimativo di soggetti interessati dalla violazione:** .....

**Misure tecniche adottate per attenuare i possibili effetti negativi della violazione:**

☐ Cifratura dei dati ☐ Copie di backup ☐ altro .....

**Probabili conseguenze della violazione:**

.....

.....

**E' stata effettuata segnalazione alle Forze di Polizia:** ☐ Si (NB allegare copia della denuncia) ☐ No

Altre notizie .....

.....

Data ..... Firma .....

**Allegato B – Scheda di valutazione della violazione dei dati personali**

## Scheda di valutazione della violazione dei dati personali (Data breach)

### Parte prima – Valutazione del Data Protection Officer

**Descrizione ed oggetto della violazione:**

……

……

**Notizie raccolte successivamente alla segnalazione pervenuta:**

……

……

**Tipo di data breach:**

□ Distruzione □ Perdita □ Modifica

□ Divulgazione non autorizzata □ Accesso non autorizzato □ Indisponibilità temporanea del dato

**Misure tecniche e organizzative applicate ai dati oggetto di violazione:**

……

……

**Persone coinvolte dalla violazione:**

□ N. certo di persone …….. □ N. presunto di persone …….. □ Numero sconosciuto

**Probabili rischi per i diritti e le libertà delle persone:**

……

……

**Livello di gravità della violazione:**

□ Basso/Trascurabile □ Medio □ Alto /Molto alto

**Azioni che si propone di intraprendere:**

□ Archiviazione

□ Notifica all'autorità di controllo

□ Comunicazione all'interessato

Per le seguenti motivazioni:

……

……

**Misure tecniche e azioni di miglioramento proposte:**

……

……

……

Data …… Il *Data Protection Officer*……

## Scheda di valutazione della violazione dei dati personali (Data breach)

**Parte seconda – Valutazione del Titolare del trattamento**

**Probabili rischi per i diritti e le libertà delle persone:**

……

……

**Livello di gravità della violazione:**

☐ Basso/Trascurabile ☐ Medio ☐ Alto /Molto alto

**Azioni e misure adottate:**

☐ Archiviazione

☐ Notifica all'autorità di controllo

Data ed estremi della notifica all'autorità di controllo: ……

……

☐ Comunicazione all'interessato

Data ed estremi della comunicazione resa all'interessato……..……..……

……

**Principali motivazioni alla base delle azioni e misure adottate:**

……..

……..

……..

**Misure tecnologiche ed organizzative adottate per contenere la violazione e prevenire analoghe future violazioni:**

……..

……..

……..

……..

**Note:**

……..

……..

……..

Data …… Il *Titolare del trattamento* ……

## Allegato C - Modello di Registro delle violazioni dei dati personali

| | REGISTRO DEI DATA BREACH DEL TITOLARE AL TRATTAMENTO DEI DATI | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| N. | Data violazione | Data segnalazione | Segnalante | Luogo della violazione | Descrizione della violazione | Dispositivo /applicativo oggetto di violazione | Categorie di dati personali | Tipologia di violazione | Categorie e numero approssimativo di soggetti interessati | Categorie e numero approssimativo di registrazioni dei dati | Probabili conseguenze della violazione | Valutazione del rischio | | | Misure e provvedimenti adottati | Notifica al Garante | | Comunicazione agli interessati | | Note e commenti |
| | | | | | | | | | | | | Alto | Medio | Basso | | SI/NO | Data | SI/NO | Data | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |