07/11/2019

ASL LATINA
UOC Affari Generali e Controllo Interno
Team Privacy

Procedura Gestione delle Violazioni di Dati Personali Data Breach

SOMMARIO

MATRICE DELLA REDAZIONE E REVISIONE			
Fasi	**Responsabilità (nome/funzione)**	**Responsabilità (firma)**	**Data**
Redazione	*Paola Bellei* *Roberta Specchio* *Eliana Marussich* *(Team Privacy)* *Dr.ssa Emma Pannunzio* *Coord. Per le Politiche della Privacy*	Paola Bellei Roberta Specchio Eliana Marussich Emma Pannunzio	18.11.2019 18.11.2019 18.11.2019 18.11.2019
Approvazione	*Direttore Generale*		

I. INTRODUZIONE

A. SCOPO

La presente Procedura sulla gestione delle Violazioni di Dati Personali ("*Data Breach*") ha lo scopo di fornire indicazioni pratiche e adempimenti da eseguire in caso di Violazione dei Dati Personali.
I termini riportati con lettera iniziale maiuscola, utilizzati nella presente procedura, si riferiscono alle definizioni riportate nel GDPR e riportate per comodità nell'Allegato ALL._01 "GLOSSARIO E ACRONIMI".

B. CAMPO DI APPLICAZIONE

La presente procedura si applica all'Ente ASL Latina (infra "**Ente**") in qualità di Titolare del Trattamento dei dati personali, per tutti i settori che svolgono attività di trattamento dei dati personali nei casi in cui si verifichi una violazione o una sospetta violazione.

II. RIFERIMENTI

A. NORMATIVA DI RIFERIMENTO

La normativa di riferimento comprende oltre al Regolamento europeo in materia di Protezione dei Dati Personali, anche le altre Leggi e disposizioni normative in materia civile e penale, secondo l'ordinamento nazionale che potrebbero prevedere il ricorso ad altre Autorità competenti. In questa sede, ci si riferisce al *Regolamento Europeo per la Protezione dei Dati Personali* n. 679/2016 (GDPR) e, in particolare ai seguenti articoli:

- **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:
  1. 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;
  2. 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;
  3. 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.

B. DOCUMENTI DI RIFERIMENTO

5. Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679
6. D.Lgs.196/2003 come novellato D.Lgs.101/2018
7. Registro dei Trattamenti ex art. 30 del GDPR
8. Privacy Policies
9. Policy Strumenti IT
10. Codice dell'Amministrazione digitale (CAD) - D.Lgs testo coordinato 07/03/2005 nr.82 , aggiornato al D.Lgs.13.12.2017 n.217
11. Manuale Aziendale del Sistema di Gestione Privacy

III. TERMINI E DEFINIZIONI

Tutti i termini riportati con lettera iniziale maiuscola si riferiscono alle definizioni riportate nel Regolamento europeo sulla protezione dei Dati Personali n. 679/2016 (GDPR) e riportate per comodità nell'allegato ALL. 01 "Glossario e Acronimi".

IV. RESPONSABILITÀ/AUTORITÀ E SOGGETTI COINVOLTI

La responsabilità del seguente processo è del Titolare del Trattamento dei Dati Personali che comunica all'Autorità di controllo e agli Interessati, laddove necessario e possibile, la Violazione (*Data breach*) verificatasi.
In particolare, i soggetti che intervengono nel processo, in base ai diversi ruoli ricoperti, sono:

- LEGALE RAPPRESENTANTE/DIRETTORE GENERALE;
- SISTEMI INFORMATIVI;
- INGEGNERIA CLINICA
- DPO/RPD;
- AFFARI GENERALI ;
- DIREZIONE AMMINISTRATIVA;
- DIREZIONE SANITARIA;
- DELEGATI AL TRATTAMENTO (come da organizzazione del Sistema Privacy);
- TEAM PRIVACY AZIENDALE;
- ALTRI SOGGETTI INTERNI e/o ESTERNI.

Nelle fasi descritte di seguito sono illustrate le modalità d'intervento operativo di ciascun soggetto coinvolto.

V. DESCRIZIONE DEL PROCESSO

A. FASE 1: RACCOLTA DELLE INFORMAZIONI

1. CANALI INTERNI

Le segnalazioni interne di eventi anomali possono:

- pervenire da tutte le figure coinvolte nel sistema di gestione *privacy* (Titolare, Delegato, Responsabile Esterno, Incaricato/Autorizzato al Trattamento)
- pervenire da tutto il personale dell'Ente;
- essere inoltrate dal DPO.

2. CANALI ESTERNI

Le segnalazioni possono pervenire anche da fonti esterne, o anche dall'analisi di informazioni presenti sul Web.

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.

3. MODALITA' DI COMUNICAZIONE

Le segnalazioni, a qualunque soggetto/funzione pervengano, devono essere tempestivamente comunicate al Titolare e al DPO comunque non oltre 12/24 ore dalla conoscenza della Violazione, a mezzo PEC protocolloaoo01@ausl.latina.it e al seguente indirizzo mail: dpo@ausl.latina.it .

La presa in carico di tutte le segnalazioni è di responsabilità del gruppo/referente *privacy* indicato dal Titolare che provvederà a gestirle coinvolgendo le altre funzioni interessate secondo quanto specificato nella presente procedura.

B. FASE 2: "DATA BREACH" PRESSO L'ENTE IN QUALITÀ DI TITOLARE - ANALISI DELLE SEGNALAZIONI

1. ANALISI PRELIMINARE E ELABORAZIONE DELLA SCHEDA EVENTO

Il gruppo/referente *privacy* avvia un'analisi preliminare finalizzata alla raccolta dei Dati concernenti l'anomalia e alla compilazione della Scheda Evento (cfr. *template* A) allegata alla presente procedura, contenente tutte le informazioni raccolte:

- Data evento anomalo
- Data presunta di avvenuta Violazione
- Data e ora in cui si è avuta conoscenza della Violazione
- Fonte segnalazione
- Tipologia della 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 la circostanza (ad esempio: smarrimento di Device Mobili, etc.)
- 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.

2. 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 in cui la Violazione su Dati Personali sia accertata, il gruppo/referente *privacy*, 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 il Team Privacy supportato dalle altre funzioni interne si attiva per effettuare un raffinamento delle regole di rilevazione dei falsi positivi, comunicando via e-mail l'esito dell'analisi al Titolare e al DPO.
L'evento viene comunque inserito a cura del Team *privacy* nel Registro dei "*Data Breach*" (cfr. *template* C) in allegato alla presente procedura) nell'apposita sezione dedicata agli "eventi falsi positivi".

3. ANALISI DI SECONDO LIVELLO - SCHEDA VIOLAZIONE DATI

Per l'analisi di secondo livello è convocato il *Risk Management*, supportato e messo in contatto, tramite i diversi mezzi di comunicazione disponibili (telefono, e-mail, skype, etc.), con le seguenti strutture aziendali:

- LEGALE RAPPRESENTANTE/DIRETTORE GENERALE;
- SISTEMI INFORMATIVI;

- INGEGNERIA CLINICA
- DPO/RPD;
- AFFARI GENERALI ;
- DIREZIONE AMMINISTRATIVA;
- DIREZIONE SANITARIA;
- DELEGATI AL TRATTAMENTO (come da organizzazione del Sistema Privacy);
- TEAM PRIVACY AZIENDALE;
- ALTRI SOGGETTI INTERNI e/o ESTERNI.

In tutti casi si procede ad analizzare congiuntamente tutte le informazioni raccolte e a redigere una Scheda Violazione Dati (cfr. *template* B) allegato alla presente procedura, per le conseguenti valutazioni.

Il gruppo coinvolto 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 di Dati non autorizzata;
- accesso ai Dati personali illecito.

La Violazione deve essere valutata secondo i livelli di rischio:

- **BASSO**
- **MEDIO**
- **ALTO**
- **MOLTO ALTO**

Il rischio è 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 gruppo coinvolto deve provvedere affinché siano tempestivamente adottate misure che consentano di minimizzare le conseguenze negative della Violazione.

C. FASE 3: NOTIFICA E COMUNICAZIONE

1. NOTIFICA ALLA AUTORITÀ DI CONTROLLO

Redatta la Scheda Violazione Dati, il gruppo 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 Titolare 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 **"BASSO"**.
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:

1. descrivere, ove possibile:
   A. la natura della Violazione dei Dati Personali compresi;
   B. le categorie ed il numero approssimativo di Interessati in questione;
   C. le categorie ed il numero approssimativo di registrazioni dei Dati Personali in questione;

b) comunicare il nome e i Dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della Violazione dei Dati Personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte dell'Ente 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.

Si riporta in calce un Modello di Notifica all'Autorità di Controllo circa la Violazione dei Dati Personali (Allegato 2).

2. COMUNICAZIONE DELLA VIOLAZIONE ALL'INTERESSATO

Il Titolare, con la collaborazione del gruppo individuato, laddove la Violazione presenti un rischio per i diritti e le libertà delle persone fisiche, deve informare gli Interessati dell'evento anomalo, a norma degli artt. 33-34 del GDPR. In particolare, la comunicazione dovrà avere luogo nei casi in cui la Violazione presenti rischi classificati come ***"ALTI o MOLTO ALTI"*** nella Scheda Violazione Dati (cfr. *template* B) allegato alla presente procedura.

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 intellegibile, coincisa, trasparente, e facilmente accessibile; deve essere utilizzato un linguaggio semplice e chiaro adottando, se possibile, la stessa lingua parlata dall'Interessato.

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 dell'Ente/Società per porre rimedio alla Violazione dei Dati Personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Deve essere valutata l'opportunità o meno di 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, ad una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia.

Si riporta in calce un Modello di comunicazione all'Interessato della Violazione dei Dati Personali (Allegato I).

D. FASE 4: REGISTRAZIONE SEGNALAZIONE NEL REGISTRO DEI "DATA BREACH"

Nel Registro dei *Data Breach* (cfr. *template* C), allegato alla presente procedura, il Titolare 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 Titolare per il tramite del Team Privacy, sotto il controllo del DPO/RPD.

E. 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, laddove necessario, delle funzioni dei Sistemi informativi, con eventuale supporto da parte di altre aree funzionali.

F. "DATA BREACH" PRESSO L'ENTE O UN TERZO IN QUALITÀ DI RESPONSABILE

1. OBBLIGHI DI COMUNICAZIONE DELL' ENTE/SOCIETÀ QUANDO OPERA IN QUALITÀ DI RESPONSABILE

Quando l'Ente 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.

2. OBBLIGHI DI COMUNICAZIONE DI UN RESPONSABILE ESTERNO NEI CONFRONTI DELL'ENTE

Nel caso in cui vi sia la presenza di un terzo che agisca in qualità di Responsabile del Trattamento, al verificarsi di una Violazione dei Dati Personali, questi deve informare l'Ente (in qualità di Titolare), senza ingiustificato ritardo e non oltre le 24 ore dal momento in cui ha conoscenza della Violazione, inviando una duplice comunicazione al seguente indirizzo: PEC – protocolloaoo01@ausl.latina.it e mail - dpo@ausl.latina.it e successivamente collaborare con l'Ente per consentire allo stesso di adempiere agli obblighi previsti dalla normativa agli artt. 33 e 34 del GDPR.
Il Responsabile Esterno deve assistere l'Ente avviando un'analisi preliminare finalizzata alla raccolta dei Dati concernenti l'anomalia e fornendo supporto al Team Privacy Aziendale per la compilazione della scheda evento sulla base del modello allegato alla presente procedura e 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 Esterno 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 Esterno deve comunicarlo immediatamente all'Ente agli stessi indirizzi di cui sopra, al fine di consentire l'inserimento del'evento nella sezione "eventi falsi positivi" del Registro dei *Data Breach* (v. *template* C).
In caso contrario, il Responsabile Esterno recupera le informazioni di dettaglio sull'evento, necessarie alle analisi di secondo livello, e unitamente al Team Privacy le riporta nella Scheda Evento che deve essere inviata, possibilmente via PEC, tempestivamente e non oltre 24 ore dalla conoscenza della Violazione, al Titolare e al DPO i quali devono essere costantemente tenuti aggiornati.
L'evento deve essere inserito dall'Ente/Società in un apposito Registro dei *Data Breach* il cui modello è allegato alla presente procedura.
L'Ente, una volta ricevuta la Scheda Evento deve procedere secondo le prescrizioni di cui ai paragrafi III. C; IV;V e VI della presente procedura.

IV. ALLEGATI

- Allegato 1: "MODELLO DI COMUNICAZIONE ALL'INTERESSATO DELLA VIOLAZIONE DEI DATI PERSONALI";
- Allegato 2: "MODELLO DI NOTIFICA DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) ALL'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI;
- *Template* A: SCHEDA EVENTO;
- *Template* B: SCHEDA VIOLAZIONE DATI
- *Template* C: REGISTRO DEI DATA BREACH

Allegato 1

MODELLO DI COMUNICAZIONE ALL'INTERESSATO DELLA VIOLAZIONE DEI DATI PERSONALI

Nota: Il seguente modello illustra le modalità di comunicazione di una Violazione. Rispetto ai diversi campi indicati dovrà essere scelta l'opzione che si può riferire allo specifico caso, in base agli esempi riportati.

Secondo quanto prescritto dall'art. 34 del Regolamento Generale in materia di protezione dei dati personali RE (UE) n. 679/2016, l'**ASL Latina**, Titolare del Trattamento, con la presente è a comunicarLe, l'intervenuta Violazione dei Suoi Dati Personali (Data breach)

- che si è verificata:
  in data _____, alle ore_____;
  tra il _____e il_____;
  in un tempo non ancora determinato;
  è possibile che sia ancora in corso.

- di cui si è avuto conoscenza in 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:
   - o lettura (presumibilmente i Dati non sono stati copiati)
   - o copia (i Dati sono ancora presenti sui sistemi del Titolare)
   - o alterazione (i Dati sono presenti sui sistemi ma sono stati alterati)
   - o cancellazione (i Dati non sono più sui sistemi del Titolare e non li ha neppure l'autore della Violazione)
   - o furto (i Dati non sono più sui sistemi del Titolare e li ha l'autore della Violazione)
   - o altro _____

c. Dispositivo oggetto di Violazione, per esempio:
   - o computer
   - o rete
   - o dispositivo mobile
   - o strumento di backup
   - o documento cartaceo
   - o altro _____

d. Descrizione dei sistemi di elaborazione o di memorizzazione dei Dati coinvolti, con indicazione della loro ubicazione:

_____
_____
_____
_____
_____
_____

e. Che tipo di Dati sono oggetto di Violazione, per esempio:
   - o Dati anagrafici (nome, cognome, numero di telefono, e mail, CF, indirizzo ecc..)
   - o Dati di accesso e di identificazione (username, password, customer ID, altro)
   - o Dati personali idonei a rivelare l'origine razziale ed etnica
   - o Dati personali idonei a rivelare le convinzioni religiose
   - o Dati personali idonei a rivelare filosofiche o di altro genere
   - o Dati personali idonei a rivelare le opinioni politiche
   - o Dati personali idonei a rivelare l'adesione a partiti
   - o Dati personali idonei a rivelare sindacati,
   - o Dati personali idonei a rivelare associazioni od organizzazioni a carattere religioso
   - o Dati personali idonei a rivelare associazioni od organizzazioni a carattere filosofico
   - o Dati personali idonei a rivelare associazioni od organizzazioni a carattere politico
   - o Dati personali idonei a rivelare associazioni od organizzazioni a carattere sindacale
   - o Dati personali idonei a rivelare lo stato di salute
   - o Dati personali idonei a rivelare la vita sessuale
   - o Dati giudiziari
   - o Dati genetici
   - o Dati biometrici
   - o Copia per immagine su supporto informatico di documenti analogici
   - o Ancora sconosciuto
   - o Altro _____

B) Descrivere le probabili conseguenze della Violazione dei Dati Personali;

_____

_____

_____

C) Descrivere quali sono le misure tecnologiche ed 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 _____ [DPO, ove esistente/funzione legale /funzione competente da identificarsi] _____ ai seguenti indirizzi:

Dati di contatto:

a) nome e cognome del DPO/RPD: _____
b) indirizzo di posta elettronica: _____
c) indirizzo di posta PEC: _____
d) indirizzo posta cartacea: _____
e) numero telefonico dedicato: _____
f) numero di fax dedicato: _____

Data, Luogo _____

Il Titolare del Trattamento

_____

DPO/RPD

_____

A. SCHEDA EVENTO

SCHEDA EVENTO					
EVENTO				PROVVEDIMENTI	
DATA EVENTO		DATA E ORA DI CONOSCENZA		NOTIFICA AL GARANTE (X)	
ORA EVENTO		SEGNALANTE		SI	NO
LUOGO DELLA VIOLAZIONE		NATURA EVENTO		(inserire data di notifica)	(motivare mancata notifica)
ENTE/SOCIETA' COINVOLTO/A		N. INTERESSATI COINVOLTI			
CATEGORIE DI DATI INTERESSATI		CATEGORIE DI INTERESSATI COINVOLTI		(eventuale) COMUNICAZIONE ALL'INTERESSATO	
				SI	NO
				(inserire data di comunicazione	(motivare mancata comunicazione)
				INTERVENTI DI RIPRISTINO (RECOVERY)	
CONSEGUENZE VIOLAZIONE		SISTEMI E DISPOSITIVI COINVOLTI			
				TEMPO DI RIPRISTINO (RECOVERY)	

DESCRIZIONE ANALITICA DELL'EVENTO	ULTERIORI AZIONI DA INTRAPRENDERE

CODICE EVENTO			
DATA DI COMPILAZIONE		FIRMA	
LUOGO DI COMPILAZIONE			
DATA ULTIMA MODIFICA			

B. SCHEDA VIOLAZIONE DATI

CODICE EVENTO 1	CLASSIFICAZIONE 2	RISCHIO 3

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.

N.B. **Griglia di classificazione**

Classificazione di rischio	Codice	Gravità della Violazione	Codice	Classificazione evento
BASSO/TRASCURABILE	RISCHIO 1	BASSO/TRASCURABILE	1	Irrilevante
MEDIO	RISCHIO 2	MEDIO	2	Falso Positivo
ALTO	RISCHIO 3	ALTO	3	Rilevante
MOLTO ALTO	RISCHIO 4	MOLTO ALTO	4	Grave (Cod. 4)

C. REGISTRO DEI DATA BREACH

Il seguente format di registro potrà essere realizzato anche in formato elettronico, richiamando i seguenti campi

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

REGISTRO DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)							
n.	DATA VIOLAZIONE	N° SCHEDA EVENTO	N. INTERESSATI COINVOLTI	NOTIFICA AL GARANTE (X)		COMUNICAZIONE AGLI INTERESSATI	
1				SI	NO	SI	NO
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)
2				SI	NO	SI	NO
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)
3				SI	NO	SI	NO
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)
4				SI	NO	SI	NO
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)
5				SI	NO	SI	NO
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)

Allegato 2

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI – MODELLO DI NOTIFICA AL GARANTE

I titolari di trattamento di dati personali sono tenuti a notificare al Garante le violazioni dei dati personali (*data breach*) che comportano accidentalmente o in modo illecito la distruzione, la perdita, la modificazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, anche nell'ambito delle comunicazioni elettroniche, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati.

La notifica non deve includere i dati personali oggetto di violazione (es. non fornire i nomi dei soggetti interessati dalla violazione).
Si ricorda che chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice in materia di protezione dei dati personali (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante), salvo che il fatto non costituisca più grave reato.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Notifica di una violazione dei dati personali

(art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del d.lgs. 51/2018)

Tipo di notifica

○ Preliminare[1] ○ Completa ◉ Integrativa [2] rif.

Effettuata ai sensi del ◉ art. 33 RGPD ○ art. 26 d.lgs 51/2018

Sez. A - Dati del soggetto che effettua la notifica

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B - Titolare del trattamento

Denominazione[3]:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Stato:
Indirizzo:
CAP : Città: Provincia:
Telefono:
E-mail:
PEC:

1 Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione con riserva di effettuare una successiva notifica integrativa. E' obbligatoria la compilazione delle sezioni A, B, B1 e C.
2 Il titolare del trattamento integra una precedente notifica (inserire il numero di fascicolo assegnato alla precedente notifica, se noto)
3 Indicare nome e cognome nel caso di persona fisica

Sez. B1- Dati di contatto per informazioni relative alla violazione

Indicare i riferimenti del soggetto da contattare per ottenere maggiori informazioni circa la violazione

◉ Responsabile della protezione dei dati[4] - prot. n.

○ Altro soggetto[5]

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B2- Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare o responsabile del trattamento[6], rappresentante del titolare non stabilito nell'Ue)

Denominazione[7] *:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile ○ Rappresentante

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

[4] Qualora designato, indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD
[5] In assenza di un RPD, indicare i riferimenti di un punto di contatto designato per la notifica in questione
[6] In tale tipologia rientra anche il Responsabile individuato ai sensi art. 28, par. 4
[7] Indicare nome e cognome nel caso di persona fisica

Sez. C - Informazioni di sintesi sulla violazione

1. **Indicare quando è avvenuta la violazione**

- (•) Il
- ( ) Dal (la violazione è ancora in corso)
- ( ) Dal al
- ( ) In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. **Momento in cui il titolare del trattamento è venuto a conoscenza della violazione**

Data: Ora:

3. **Modalità con la quale il titolare del trattamento è venuto a conoscenza della violazione**

- ( ) Il titolare è stato informato dal responsabile del trattamento
- ( ) Altro[8]

4. **In caso di notifica oltre le 72 ore, quali sono i motivi del ritardo?[9]**

5. **Breve descrizione della violazione**

[8] Ad esempio: Segnalazione da parte di un interessato, comunicazione da parte di terzi, ecc.

[9] Da compilare solo per notifiche tardive.

6. **Natura della violazione**
   - ☐ a) Perdita di confidenzialità[10]
   - ☐ b) Perdita di integrità[11]
   - ☐ c) Perdita di disponibilità[12]

7. **Causa della violazione**
   - ☐ Azione intenzionale interna
   - ☐ Azione accidentale interna
   - ☐ Azione intenzionale esterna
   - ☐ Azione accidentale esterna
   - ☐ Sconosciuta
   - ☐ Altro (specificare)

8. **Categorie di dati personali oggetto di violazione**
   - ☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
   - ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
   - ☐ Dati di accesso e di identificazione (username, password, customer ID, altro…)
   - ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
   - ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
   - ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
   - ☐ Dati di profilazione
   - ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
   - ☐ Dati di localizzazione
   - ☐ Dati che rivelino l'origine razziale o etnica
   - ☐ Dati che rivelino opinioni politiche
   - ☐ Dati che rivelino convinzioni religiose o filosofiche
   - ☐ Dati che rivelino l'appartenenza sindacale
   - ☐ Dati relativi alla vita sessuale o all'orientamento sessuale
   - ☐ Dati relativi alla salute
   - ☐ Dati genetici
   - ☐ Dati biometrici
   - ☐ Categorie ancora non determinate
   - ☐ Altro

[10] Diffusione/ accesso non autorizzato o accidentale
[11] Modifica non autorizzata o accidentale
[12] Impossibilità di accesso,perdita, distruzione non autorizzata o accidentale

9. Indicare il volume (anche approssimativo) dei dati personali oggetto di violazione[13]

- ○ N.
- ○ Circa n.
- ○ Un numero (ancora) non definito di dati

10. Categorie di interessati coinvolti nella violazione

- ☐ Dipendenti/Consulenti
- ☐ Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
- ☐ Associati,soci, aderenti, simpatizzanti, sostenitori
- ☐ Soggetti che ricoprono cariche sociali
- ☐ Beneficiari o assistiti
- ☐ Pazienti
- ☐ Minori
- ☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
- ☐ Categorie ancora non determinate
- ☐ Altro (specificare)

☐ Ulteriori dettagli circa le categorie di interessati

11. Numero (anche approssimativo) di interessati coinvolti nella violazione

- ○ N. interessati
- ○ Circa n. interessati
- ○ Un numero (ancora) sconosciuto di interessati

[13] Ad esempio numero di referti, numero di record di un database, numero di transazioni registrate.

Sez. D - Informazioni di dettaglio sulla violazione

1. **Descrizione dell'incidente di sicurezza alla base della violazione**[14]

2. **Descrizione delle categorie di dati personali oggetto della violazione**[15]

3. **Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione**

4. **Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti**[16]

[14] Segue punto 5, 6 e 7 della sez. C
[15] Segue punto 8 della sez. C
[16] Indicare le misure in essere al momento della violazione

Sez. E - Possibili conseguenze e gravità della violazione

1. Possibili conseguenze della violazione sugli interessati

a) In caso di perdita di confidenzialità: [17]

☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
☐ Altro (specificare)

b) In caso di perdita di integrità:[18]

☐ I dati sono stati modificati e resi inconsistenti
☐ I dati sono stati modificati mantenendo la consistenza
☐ Altro (specificare)

c) In caso di perdita di disponibilità:[19]

☐ Mancato accesso a servizi
☐ Malfunzionamento e difficoltà nell'utilizzo di servizi
☐ Altro (specificare)

Ulteriori considerazioni sulle possibili conseguenze

[17] Da compilare solo nel caso in cui è stata selezionata l'opzione a) del punto 6, Sez. C
[18] Da compilare solo nel caso in cui è stata selezionata l'opzione b) del punto 6, Sez. C
[19] Da compilare solo nel caso in cui è stata selezionata l'opzione c) del punto 6, Sez. C

2. **Potenziali effetti negativi per gli interessati**

☐ Perdita del controllo dei dati personali
☐ Limitazione dei diritti
☐ Discriminazione
☐ Furto o usurpazione d'identità
☐ Frodi
☐ Perdite finanziarie
☐ Decifratura non autorizzata della pseudonimizzazione
☐ Pregiudizio alla reputazione
☐ Perdita di riservatezza dei dati personali protetti da segreto professionale
☐ Conoscenza da parte di terzi non autorizzati
Qualsiasi altro danno economico o sociale significativo (specificare)

3. **Stima della gravità della violazione**

○ Trascurabile
○ Basso
○ Medio
○ Alto

Indicare le motivazioni

Sez. F – Misure adottate a seguito della violazione

1. **Misure tecniche e organizzative adottate (o di cui si propone l'adozione[20]) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati**

2. **Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future**

[20] Nella descrizione distinguere le misure adottate da quelle in corso di adozione

Sez. G - Comunicazione agli interessati

1. La violazione è stata comunicata agli interessati?

- ○ Sì, è stata comunicata il
- ○ No, sarà comunicata
  il
  in una data da definire
- ○ No, sono tuttora in corso le dovute valutazioni[21]
- ◉ No e non sarà comunicata perché:
  a) il titolare del trattamento ritiene che la violazione dei dati personali non presenti un rischio elevato per i diritti e le libertà delle persone fisiche;
  Spiegare le motivazioni

  b) 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;

  Descrivere le misure applicate

  ■ c) 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;

  Descrivere le misure adottate

  d) detta comunicazione richiederebbe sforzi sproporzionati.
  Descrivere la modalità (comunicazione pubblica o misura simile) tramite la quale gli interessati sono stati informati

[21] Selezionando questa opzione, il titolare del trattamento si impegna a effettuare una integrazione alla presente notifica

2. **Numero di interessati a cui è stata comunicata la violazione**[22]

   N. interessati

3. **Contenuto della comunicazione agli interessati**

4. **Canale utilizzato per la comunicazione agli interessati**
   - ☐ SMS
   - ☐ Posta cartacea
   - ☐ Posta elettronica
   - ☐ Altro (specificare)

[22] Da compilare solo nel caso in cui al punto 1 venga scelta una delle prime due opzioni.

Sez. H - Altre informazioni

1. **La violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo[23]?**

   ◉ SI (indicare quali):

   ○ NO

2. **La violazione coinvolge interessati di Paesi non appartenenti allo Spazio Economico Europeo?**

   ○ SI (indicare quali):

   ○ NO

3. **La violazione è stata notificata ad altre autorità di controllo[24]?**

   ○ SI (indicare quali):

   ○ NO

4. **La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[25]?**

   ○ SI (indicare quali):

   ○ NO

5. **E' stata effettuata una segnalazione all'autorità giudiziaria o di polizia?**

   ○ SI
   ○ NO

[23] Fanno parte dello Spazio Economico Europeo tutti gli Stati membri della Unione Europea, nonchè l'Islanda, il Liechtenstein e la Norvegia
[24] Autorità di controllo così come definite ex art. 51 del Regolamento (UE) 2016/679
[25] Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Garante per la protezione dei dati personali, in qualità di titolare del trattamento (con sede in Piazza Venezia 11, IT-00187, Roma; Email: garante@gpdp.it; PEC: protocollo@pec.gpdp.it; Centralino: +39 06696771), tratterà i dati personali conferiti con il presente modulo, con modalità prevalentemente informatiche e telematiche, per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e s.m.i.), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri attribuiti al Garante dalla disciplina vigente.

Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio e la loro mancata indicazione non consente di ritenere adempiuto il dovere di notificazione della violazione all'autorità di controllo. I dati acquisiti nell'ambito della procedura saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa.

I dati saranno trattati esclusivamente dal personale e da collaboratori del Garante o delle imprese espressamente designate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

Gli interessati hanno il diritto di ottenere dal Garante, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento UE 2016/679). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati presso il Garante (Garante per la protezione dei personali - Responsabile della Protezione dei dati personali, Piazza Venezia 11, 00187, Roma, email: rpd@gpdp.it).

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dalla disciplina in materia di protezione dei dati personali hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento (UE) 2016/679, o di adire le opportune sedi giudiziarie ai sensi dell'art. art. 79 del Regolamento citato.