A.S.L. V.C.O.
Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

DELIBERAZIONE DEL DIRETTORE GENERALE

N. 683 del 07/08/2025

Oggetto: AGGIORNAMENTO PROCEDURA PER LA GESTIONE DELLE SEGNALAZIONI DI VIOLAZIONE DEI DATI (DATA BREACH).

DIRETTORE GENERALE - DOTT. FRANCESCO CATTEL
(NOMINATO CON DGR N. 25-655/2024/XII DEL 23/12/2024)

DIRETTORE SANITARIO - DOTT.SSA DANIELA KOZEL

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

DELIBERAZIONE DEL DIRETTORE GENERALE

Struttura proponente: AFFARI GENERALI LEGALI E ISTITUZIONALI

L'estensore dell'atto: Motetta Emanuela
Il Responsabile del procedimento: Primatesta Giuseppina
Il Dirigente/Funzionario: Priolo Vittoria Maria
Il funzionario incaricato alla pubblicazione.

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

IL DIRETTORE GENERALE

Nella data sopraindicata, su proposta istruttoria del Direttore SOC Affari Generali Legali e Istituzionali – SOS Organi Organismi Collegiali Supporto Strategico - di seguito riportata, in conformità al Regolamento approvato con delibera n. 290 del 12/05/2017 e modificato con delibere n. 65 del 28/01/2020 e n. 555 del 25/06/2025.

"PREMESSO CHE

- il Regolamento (UE) 2016/679 del Parlamento e del Consiglio Europeo del 27 aprile 2016 (GDPR) disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali ;
- l'art. 33 del suddetto GDPR 2016/679 così dispone: "In caso di violazioni di dati personali, il Titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 55, senza ingiustificato ritardo e, ove possibile, entro le 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";

- le Linee Guida del Gruppo ex art. 29 n. 250 del 3 ottobre 2017, emendate in data 6 febbraio 2018, illustrano gli obblighi di notifica e di comunicazione in caso di violazioni dei dati personali, ai sensi del Regolamento EU 2016/679 e forniscono inoltre alcuni esempi di vari tipi di violazioni;

- il Decreto Legislativo 10 agosto 2018, n. 101, disciplina l'adeguamento della normativa italiana al Regolamento (UE) 2016/679 (GDPR) in materia di protezione dei dati personali. In particolare, il decreto modifica il Codice della Privacy (Decreto Legislativo 30 giugno 2003, n. 196), armonizzandolo con le disposizioni del GDPR.

DATO ATTO che per "Data Breach" si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali" e cioè, nello specifico, una 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 mancata notifica può comportare ulteriori accertamenti da parte del Garante, poiché può rappresentare un indizio di carenze che, se accertate, possono dar luogo a sanzioni e, pertanto, tutti gli eventi di Data Breach, compresi quelli per cui la notifica non è necessaria, devono essere documentati in un "Registro delle Violazioni" (art. 33 paragrafo 5 RGPD).

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

PRESO ATTO che in caso di violazione dei dati personali, il titolare del trattamento è tenuto a notificare tale evento al Garante 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 (art. 33 del GDPR).

PRESO ATTO altresì che il titolare del trattamento è tenuto a notificare la violazione dei dati personali al Garante con le modalità di cui all'art. 33 del GDPR anche con riferimento al trattamento effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvo che il trattamento medesimo sia effettuato dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero (artt. 26 e 37, comma 6, del D.lgs. n. 51/2018).

RILEVATO che, ai sensi della Direttiva UE 2022/2555 (cosiddetta Direttiva NIS 2), come recepita nel D.Lgs 138/2024, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati, anche se non coinvolgono dati personali, devono comunque essere notificati senza indebito ritardo al CSIRT (Computer Security Incident Response Team - Gruppo di intervento per la sicurezza informatica in caso di incidente) e all'autorità NIS competente, cioè ACN.
Per la Direttiva NIS si definisce incidente "*ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi*". In questo caso, quindi, si sovrappongono le due normative e l'Azienda sanitaria che eroga il servizio interessato dall'incidente (e dalla contestuale violazione dei dati personali) deve adempiere agli obblighi di notifica previsti da entrambe le normative, ossia deve effettuare sia la notifica per gli incidenti di cui alla Direttiva NIS, sia la notifica per la violazione dei dati personali prevista dal GDPR.

DATO ATTO che le comunicazioni inerenti gli incidenti informatici sopra citati sono di competenza del Punto di Contatto della azienda registrato presso il portale ACN, in quanto tale soggetto – secondo le disposizioni dell'articolo 25 del d.lgs. n. 138/2024 - ha il compito di curare l'attuazione delle disposizioni del decreto NIS per conto del soggetto stesso, a partire dalla registrazione, e interloquisce, per conto del soggetto NIS, con l'Autorità nazionale competente NIS.

RILEVATO CHE che, nell'organigramma allegato all'Atto Aziendale vigente, approvato con deliberazione DG n. 602 del 18/08/2022, è presente la Funzione Privacy, collocata nell'ambito della SOC Affari Generali Legali e Istituzionali, in staff alla Direzione Generale, che, con il supporto del Responsabile per la Protezione dei dati (o DPO), ha il compito di supportare il Titolare del Trattamento Dati (ASL VCO – nella persona del legale rappresentante), nella gestione degli adempimenti inerenti la tutela dei dati personali.

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

VISTE

- la deliberazione D.G. n. 831 in data 10/8/2018 con la quale, in applicazione dell'art. 33 del Regolamento UE 2016/679 in materia di privacy (GDPR), veniva approvata la procedura da porre in essere in caso di "Data breach", alla quale risultava allegato il modello per effettuare la notifica al Garante della Privacy, reso disponile dal Garante medesimo;

- la deliberazione D.G. n. 787 del 16/10/2019 con la quale si procedeva alla modifica della procedura approvata con la deliberazione sopra citata, aggiornando l'allegato modello di notifica notifica di "Data breach", in applicazione del Provvedimento del Garante Privacy n. 157 del 30/7/2019.

PRESO ATTO che, con Provvedimento del 27 maggio 2021, il Garante per la Protezione dei Dati Personali ha modificato le modalità di notifica dei Data breach adottando la "Procedura telematica per la notifica di violazioni di dati personali" .

RILEVATO CHE la Funzione Privacy sopra citata, tenuto conto delle successive modifiche intervenute nell'ambito dell'organizzazione dell'Azienda ed a livello normativo/regolamentare, ha provveduto ad aggiornare la procedura in oggetto ed a trasmetterla al Responsabile della Protezione Dati, il quale l'ha esaminata senza rilievi.

RITENUTO pertanto di formalizzare la procedura allegata alla presente deliberazione sotto la lettera A) , alla quale risultano uniti i seguenti allegati:

- A1 Schema di valutazione scenari – data breach
- A2 Fac-simile modello di notifica al Garante (tramite procedura telematica)

Condivisa la proposta come sopra formulata e ritenendo sussistere le condizioni per l'assunzione della presente delibera.

Acquisiti i pareri favorevoli espressi ai sensi dell'art. 3 del d.Lgs. 502/1992 e smi, come formulati nel frontespizio del presente atto

DELIBERA

1°) Di approvare l'aggiornamento della Procedura per la Gestione delle Segnalazioni di Violazione dei Dati (Data Breach) ai sensi dell'art. 33 del GDPR 2016/679, che viene allegata alla presente deliberazione quale parte integrante e sostanziale sotto la lettera A), comprensiva dei seguenti sub-allegati:
- A1 Schema di valutazione scenari – data breach
- A2 Fac-simile modello di notifica al Garante (tramite procedura telematica)

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

2°) Di dare atto che la procedura di cui al punto 1° sostituisce integralmente quella precedentemente approvata con deliberazioni DG nn. 831/2018 e 787/2019.

3°) Di precisare che le comunicazioni inerenti gli incidenti informatici ai sensi della Direttiva UE 2022/2555 (cosiddetta Direttiva NIS 2), come recepita nel D.Lgs 138/2024, sono di competenza del Punto di Contatto dell'azienda registrato presso il portale ACN, in quanto tale soggetto, come previsto dall'articolo 25 del D.lgs. citato, ha il compito di curare l'attuazione delle disposizioni del decreto NIS 2.

4°) Di disporre, a cura della Funzione Privacy aziendale, la pubblicazione del presente atto, unitamente alla procedura ed ai suoi allegati, sul sito intranet aziendale – Aree tematiche - sezione Privacy, nonché la notifica a tutte le strutture aziendali.

5°) Di dare atto che il presente provvedimento non comporta alcun onere di spesa a carico del bilancio dell'Azienda.

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

ALLEGATO A)

PROCEDURA PER LA GESTIONE DELLE SEGNALAZIONI DI VIOLAZIONE DEI DATI (DATA BREACH)

(ART. 33 REGOLAMENTO UE 2016/679 IN MATERIA DI PRIVACY)

(AGGIORNAMENTO AGOSTO 2025)

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it
P.I./Cod.Fisc. 00634880033

Indice

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

PREMESSA

La procedura illustra le azioni da compiere in caso di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti interessati o di incidenti rilevanti, a chi devono essere comunicate e in che modo, secondo le disposizioni del Regolamento UE 2016/679 in materia di protezione dei dati personali.

La Procedura tiene conto delle Linee Guida del Gruppo ex art. 29 n. 250 del 3 ottobre 2017, emendate in data 6 febbraio 2018 (che illustrano gli obblighi di notifica e di comunicazione in caso di violazioni dei dati personali, ai sensi del Regolamento EU 2016/679), e del D.Lgs. 138/2024 che recepisce la Direttiva UE 2022/2555 (c.d. Direttiva NIS 2), avente ad oggetto il "*Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148".*

A. DATA BREACH (Violazione dei dati)

L'art. 33 del GDPR recita che: "In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 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".
Ai sensi dell'art. 4 punto 12 del GDPR per "Violazione di dati personali" (Data breach) 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".
Le Linee Guida del Gruppo ex art. 29 n. 250 del 3 ottobre 2017, emendate in data 6 febbraio 2018, illustrano gli obblighi di notifica e di comunicazione in caso di violazioni dei dati personali, ai sensi del Regolamento EU 2016/679 e forniscono inoltre alcuni esempi di vari tipi di violazioni.
Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro sopra citato ha spiegato che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni:

- "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.

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

La mancata notifica può comportare ulteriori accertamenti da parte del Garante poiché può rappresentare un indizio di carenze che, se accertate, possono dar luogo a sanzioni.

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it
P.I./Cod.Fisc. 00634880033

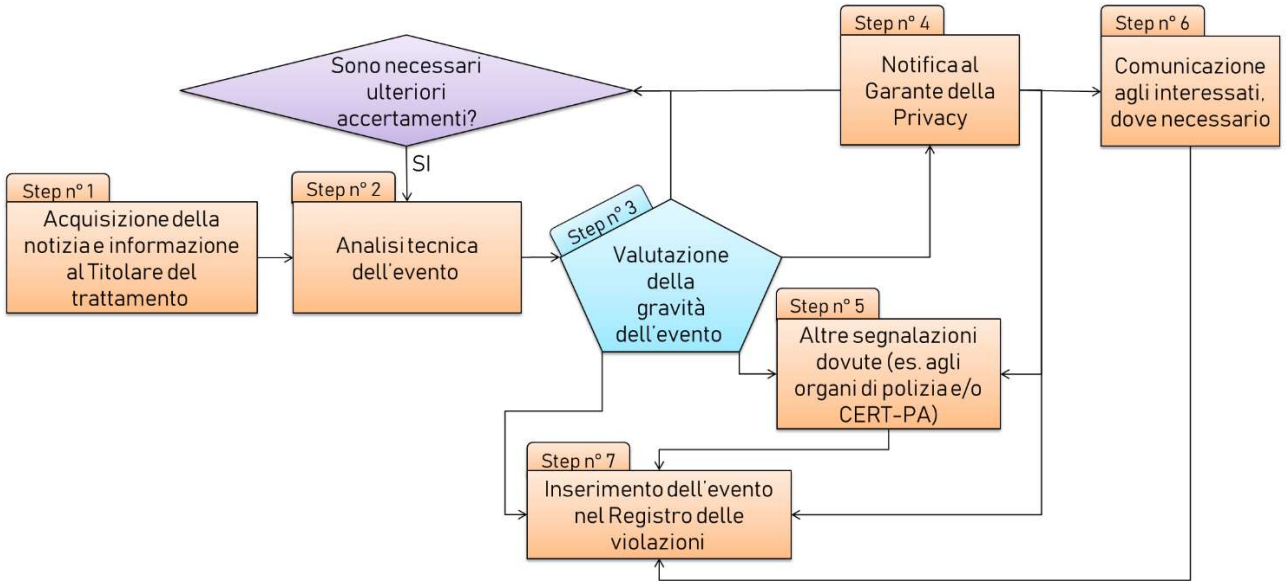
Tutti gli eventi di Data Breach, compresi quelli per cui non sono necessarie le notifiche, devono essere documentati (art. 33 par. 5 del GDPR) su un Registro delle Violazioni.

Allo scopo di supportare i soggetti coinvolti nella valutazione in merito alla necessità di effettuare o meno la notifica di data breach all'Autorità Garante, nell'allegato 1) alla presente procedura (Schema di valutazione scenari – data breach) vengono illustrati alcuni esempi, non esaustivi, di possibili violazioni di dati personali.

B. PROCESSO DI DATA BREACH NOTIFICATION

In caso di accertamento di violazione dei sistemi informatici, di involontaria diffusione delle informazioni o di altri eventi che rientrano nella definizione di Data Breach, sarà opportuno seguire i seguenti steps del processo di notificazione (rappresentati nel relativo schema):

1. Acquisizione della notizia e informazione al Titolare del trattamento
2. Analisi tecnica dell'evento
3. Valutazione della gravità dell'evento
4. Notifica al Garante della Privacy
5. Altre segnalazioni dovute
6. Comunicazione agli interessati (dove necessario)
7. Inserimento dell'evento nel Registro delle Violazioni



Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it
P.I./Cod.Fisc. 00634880033

1. Acquisizione della notizia e informazione al Titolare del trattamento
La segnalazione di un Data Breach può essere interna o esterna all'Ente.

• INTERNAMENTE:
o Dal settore dei Sistemi Informativi
o Da altro personale interno
Le segnalazioni interne di eventi anomali e/o presunte violazioni possono pervenire dal personale interno all'Azienda (settore sistemi informativi, dipendenti o personale convenzionato/stagisti/tirocinanti, ecc.); in questo caso il soggetto deve segnalare l'accaduto al rispettivo designato (coincidente con il Direttore/Responsabile della struttura di afferenza), il quale, deve comunicare alla Funzione Privacy Aziendale la presunta violazione inviando una mail a privacy@aslvco.it, allegando eventuale documentazione correlata e fornendo breve relazione contenente gli elementi necessari ad effettuare l'analisi tecnica dell'evento per determinarne la gravità e l'eventuale necessità di notifica al Garante.

Tale comunicazione deve essere fatta entro le 12 ore dalla conoscenza della presunta violazione.
La funzione privacy aziendale provvederà quindi all'inoltro della segnalazione alla pec aziendale per la protocollazione.
• ESTERNAMENTE:
o Da parte degli organi pubblici (Agid, Polizia, altre forze dell'ordine, giornali, ecc.)
o Da parte di Responsabili al trattamento
o Da parte degli interessati

Le segnalazioni da parte di fonti esterne possono pervenire direttamente alla PEC aziendale (protocollo@pec.aslvco.it), alla casella del dpo (dpo@aslvco.it), o all'U.R.P. (urp@aslvco.it). Nel caso in cui le segnalazioni pervengano all'URP o al dpo questi provvederanno ad inoltrarle alla pec aziendale per l'acquisizione al protocollo e contestualmente darne comunicazione telefonica all'ufficio privacy aziendale.

Qualora la segnalazione esterna dovesse pervenire alla mail della struttura direttamente coinvolta, quest'ultima provvederà ad inoltrarla alla pec aziendale e contestualmente darne comunicazione telefonica all'ufficio privacy aziendale.

L'Ufficio privacy provvederà, non appena ricevuta notizia dell'evento, ad informare il Titolare.
Dal momento in cui il Titolare viene a conoscenza dell'evento (data di acquisizione del documento al protocollo ufficiale), decorre il termine di 72 ore previsto dalla normativa per l'invio della notifica all'autorità di controllo.

2. Analisi tecnica dell'evento
Il Titolare è responsabile della valutazione e relativa notifica e sarà supportato dai soggetti interni all'Azienda preposti a tale attività. In primo luogo dal Referente Privacy (afferente alla Funzione "Corruzione/Trasparenza/Privacy", collocata nell'ambito della SOC Affari

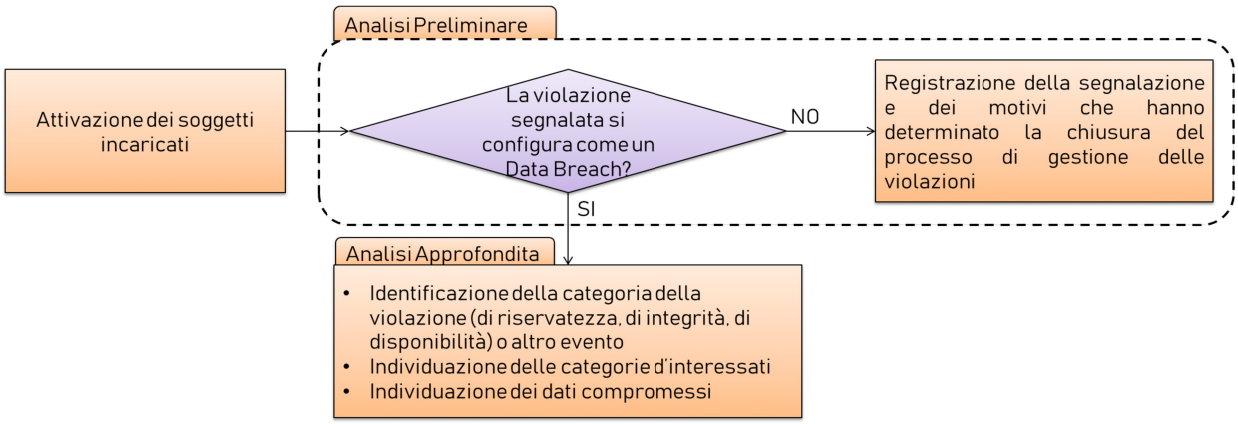
Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it
P.I./Cod.Fisc. 00634880033

Generali Legali e Istituzionali, in staff alla Direzione Generale), il quale, provvederà a coinvolgere il Responsabile della Protezione Dati ed i soggetti Designati, per quanto di competenza.

Nel caso di incidenti informatici l'analisi tecnica ed i conseguenti adempimenti relativi alla cybersicurezza vengono effettuati dalla SOS ICT (Information Comunication Technologies - Tecnologia dell'Informazione e della Comunicazione), con il supporto del DPO ed informando il Referente Privacy per gli adempimenti di competenza.

In particolare, una volta verificato che l'evento segnalato si configuri effettivamente come un "Data Breach" (Analisi Preliminare), verranno svolte tutte le operazioni necessarie a raccogliere gli elementi per una valutazione dell'evento (Analisi Approfondita) ai fini della notifica al Garante della Privacy.
È importante sottolineare che, anche nel caso in cui dall'Analisi Preliminare emerga che la segnalazione non ha i caratteri del Data Breach, è necessario registrarla nel Registro delle Violazioni.
Durante l'Analisi Approfondita, dovranno essere accertate le circostanze della violazione, le conseguenze e i relativi rimedi.
Si precisa che l'art. 33 paragrafo n. 4 del DGPR recita: "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".

Pertanto, sarà fondamentale raccogliere il maggior numero di informazioni e, anche in caso queste non siano per il momento ritenute esaustive, effettuare la notificazione.
Nello specifico verrà effettuato, in un tempo consigliabile non superiore a 8-10 ore:
- Il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità) o altro evento
- L'identificazione dei dati violati/distrutti/compromessi
- L'identificazione degli interessati



Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it
P.I./Cod.Fisc. 00634880033

3. Valutazione della gravità dell'evento

Il Titolare è responsabile anche di questa fase, in cui dovrà appurare se l'evento merita di essere notificato al Garante della Privacy e, insieme ai soggetti interni di ausilio alla fase di analisi tecnica (in primo luogo il Referente Privacy), dovrà:

- informare il DPO
- accertare la probabilità o meno che l'evento abbia comportato dei rischi per i diritti e la libertà delle persone (cioè quando si è verificata una distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati, sia che questi dati siano trattati all'interno che all'esterno dell'ente)
- effettuare la notifica al Garante, se necessaria
- verificare, successivamente, se sia necessaria una seconda notifica più approfondita, di conseguenza ad un'analisi tecnica supplementare
- effettuare una comunicazione agli organi di polizia, se necessaria (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti).

L'art. 33 paragrafo n. 1 chiarisce che non vi è obbligo di notifica della violazione al Garante quando è "improbabile" che questa comporti un rischio per i diritti e le libertà delle persone fisiche, ovviamente il giudizio che determina l'improbabilità del rischio deve essere riportato nel Registro delle violazioni.

4. Notifica al Garante della Privacy

Come accennato, la notifica di una violazione al Garante è resa obbligatoria dall'art. 33 del GDPR nei casi in cui si verifichi una violazione dei dati personali, a meno che sia improbabile che tale violazione presenti un rischio per i diritti e le libertà delle persone fisiche.

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ in attuazione del Provvedimento del Garante del 27 maggio 2021. Nella stessa pagina è disponibile un modello facsimile, da utilizzare unicamente per visualizzare in anteprima i contenuti che andranno comunicati al Garante (All. 2 alla presente procedura).

La notifica è effettuata, su delega del Titolare, dal Referente Privacy, o, in sua assenza, dal Direttore della SOC Affari Generali legali e istituzionali.

La notifica, come previsto dalla procedura sopra citata, prevede i seguenti elementi:

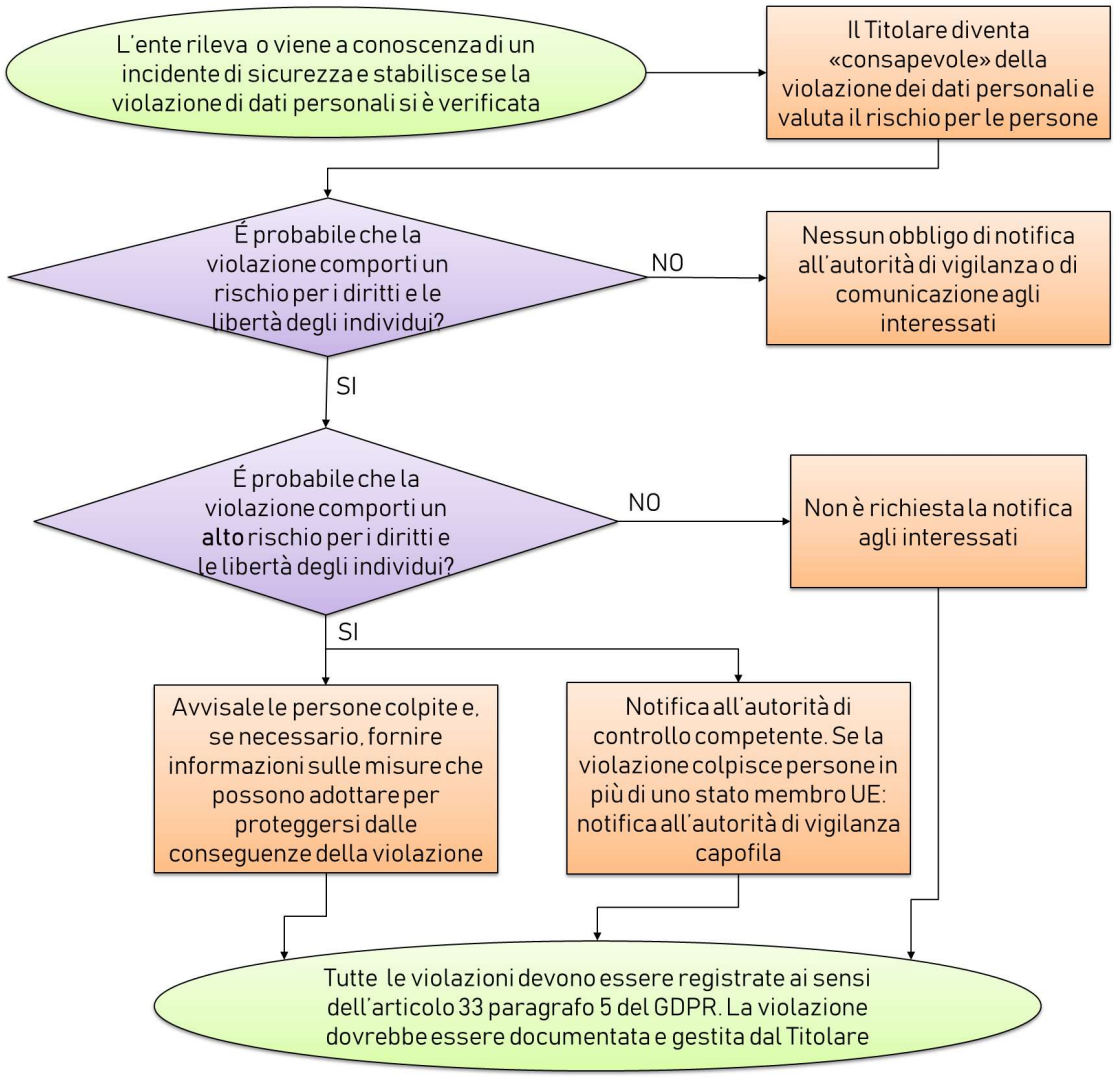
- La descrizione della violazione dei dati personali compresi, ove possibile le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione
- Dati del soggetto che effettua la notifica
- Tipo di notifica (prima notifica o notifica integrativa)
- Motivo dell'integrazione (se notifica integrativa)

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

- Titolare del Trattamento e relativi dati
- Dati di contatto per informazioni relative alla violazione (Responsabile della Protezione Dati)
- Ulteriori soggetti coinvolti nel trattamento
- Informazioni sulla violazione (momento in cui è avvenuta la violazione, modalità con la quale il Titolare è venuto a conoscenza della violazione, momento in cui il Titolare è venuto a conoscenza della violazione)
- Motivi del ritardo (nel caso in cui la notifica venga fatta oltre i termini)
- Natura della violazione
- Causa della violazione
- Descrizione della violazione
- Descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione
- Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti
- Categorie e numero di interessati coinvolti nella violazione
- Categorie di dati personali oggetto di violazione
- Numero (anche approssimativo) di registrazioni dei dati personali oggetto di violazione
- Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati
- Probabili conseguenze della violazione per gli interessati, potenziale impatto per gli interessati e gravità del potenziale impatto
- Misure adottate a seguito della violazione
- Valutazione del rischio per gli interessati
- Comunicazione della violazione agli interessati (con indicazione del numero degli interessati, del canale utilizzato e del contenuto della comunicazione)
- Altre informazioni (eventuali ulteriori notifiche a organismi di vigilanza o di controllo, autorità giudiziaria o di polizia)
- Informazioni relative a violazioni transfrontaliere e relative notifiche effettuate.

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it
P.I./Cod.Fisc. 00634880033



5. Altre segnalazioni dovute

Il Titolare dovrà verificare la necessità di informare altri organi quali:
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti);

- Notificazione di incidenti informatici rilevanti

Ai sensi della Direttiva UE 2022/2555 (cosiddetta Direttiva NIS 2), come recepita nel D.Lgs 138/2024, gli incidenti che rientrano nella categoria prevista e comportano un impatto rilevante sulla continuità dei servizi essenziali prestati, anche se non coinvolge dati personali, devono comunque essere notificati senza indebito ritardo anche al CSIRT (Computer Security Incident Response Team - Gruppo di intervento per la sicurezza informatica in caso di incidente) e all'autorità NIS competente, cioè ACN.

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it
P.I./Cod.Fisc. 00634880033

Per la Direttiva NIS si definisce incidente "ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi".
In questo caso, quindi si sovrappongono le due normative e l'Azienda sanitaria che eroga il servizio interessato dall'incidente (e dalla contestuale violazione dei dati personali) deve adempiere agli obblighi di notifica previsti da entrambe le normative, ossia deve effettuare sia la notifica per gli incidenti di cui alla Direttiva NIS, sia la notifica per la violazione dei dati personali prevista dal GDPR.

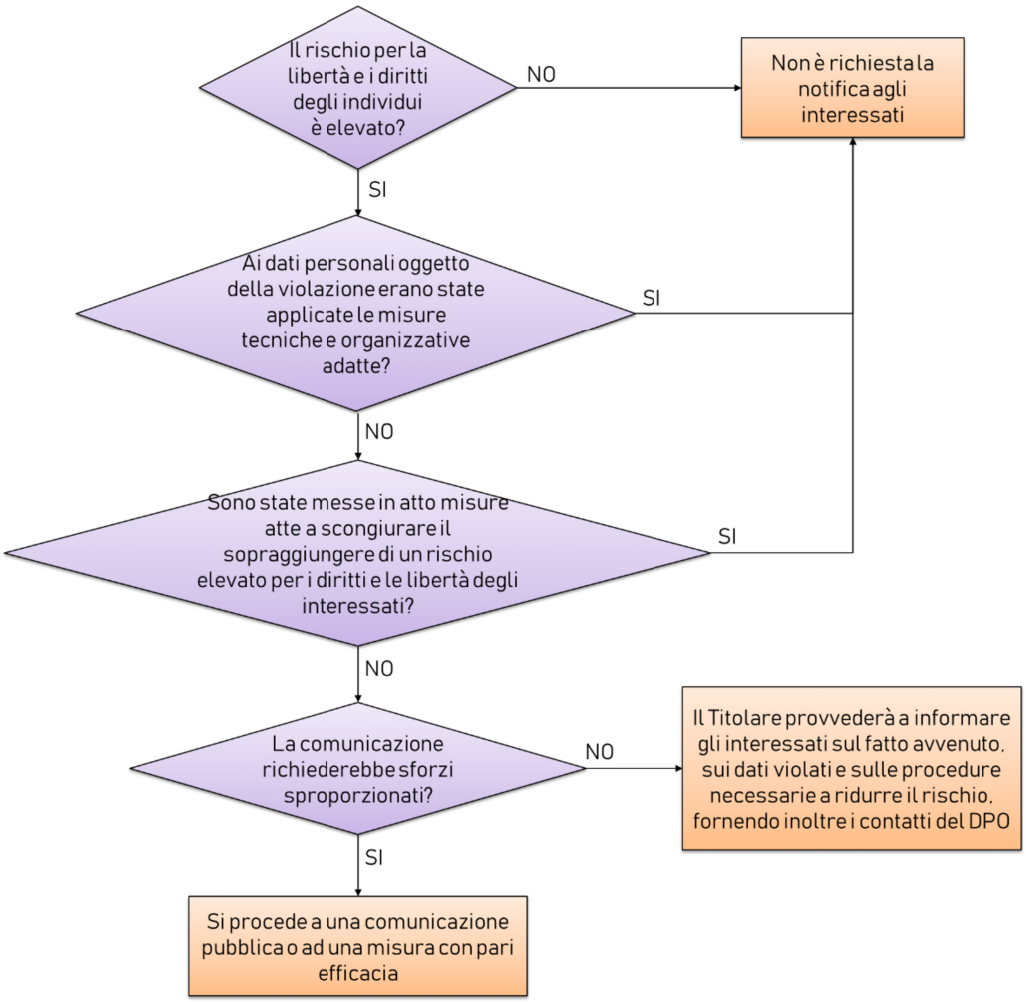
Tali comunicazioni sono di competenza del Punto di Contatto della azienda registrato presso il portale ACN, in quanto tale soggetto – secondo le disposizioni dell'articolo 25 del d.lgs. n. 138/2024 - ha il compito di curare l'attuazione delle disposizioni del decreto NIS per conto del soggetto stesso, a partire dalla registrazione, e interloquisce, per conto del soggetto NIS, con l'Autorità nazionale competente NIS.

6. Comunicazione agli interessati

In caso di elevato rischio per la libertà e i diritti degli individui, il Titolare provvederà a informare gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio.
La comunicazione agli interessati, secondo quanto previsto dal paragrafo n. 3 dell'art. 34 del GDPR, non è richiesta quando:
- 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;
- 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;
- 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.

La comunicazione deve contenere, ai sensi dell'art. 34, le seguenti informazioni:
- il nome e i dati di contatto del DPO o di altro punto di contatto;
- 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 anche, se del caso, per attenuarne i possibili effetti negativi.

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it
P.I./Cod.Fisc. 00634880033



7. Inserimento dell'evento nel Registro delle violazioni

L'art. 33 Paragrafo n.5 del GDPR, prescrive al Titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

Il registro delle violazioni in Azienda è gestito tramite l'apposito applicativo utilizzato per gli adempimenti privacy.

Pertanto, tutte le attività indicate sopra, devono essere documentate, tracciabili, ed essere in grado di fornire evidenza nelle sedi competenti.
Tale procedura deve essere diffusa a tutti i soggetti deputati al trattamento dei dati personali che, a diverso titolo, potranno e dovranno essere di ausilio al Titolare del trattamento.

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it
P.I./Cod.Fisc. 00634880033

Il DPO dovrà essere informato dal Titolare del trattamento, come indicato sopra, dovrà inoltre configurarsi come punto di contatto delle comunicazioni tra Garante e Titolare.

8. Azioni di miglioramento

Il Titolare, sulla base dell'analisi delle violazioni riportate nel Registro delle violazioni, provvederà a documentare le azioni di miglioramento messe in atto, tra le quali è ricompresa l'individuazione di verifiche e audit mirati alla riduzione delle probabilità di possibili violazioni di dati personali.

[redacted] Schema di valutazione scenari – data breach

Di seguito sono illustrati alcuni esempi, non esaustivi, di possibili violazioni di dati personali, allo scopo di supportare i soggetti coinvolti nella procedura, nella valutazione in merito alla necessità di effettuare o meno la notifica di data breach all'Autorità Garante.

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	• Rottura dell'ecografo prima di inviare al sistema centrale l'immagine. • Guasto non riparabile dell'hard disk contenente uno o più referti che, in violazione al regolamento, erano salvati localmente • Incendio di archivio cartaceo delle cartelle cliniche. • Distruzione di campioni biologici	• Rottura di una chiavetta USB che non contiene dati personali originali (in unica copia) • Rottura di un PC che non contiene dati personali originali (in unica copia) • Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo
Perdita	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili • Dati relativi a più assistiti, relativi a interi episodi o relativi a tipologie di dato la cui indisponibilità lede i diritti fondamentali dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamentali dell'interessato Rientrano tra i casi di	• Smarrimento di chiavetta USB contenente dati originali • Smarrimento di fascicolo cartaceo personale dipendente	• Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa

[redacted]

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
		segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione		
Modifica	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	Caratteristiche: • Modifiche sistematiche su più casi Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Guasto tecnico che altera parte dei contenuti di un sistema clinico, compromettendo anche i backup • Azione involontaria, o fraudolente, di un utente che porta alla alterazione di dati sanitari in modo non tracciato e irreversibile	• Guasto tecnico che altera parte dei contenuti di un sistema clinico, rilevato e sanato tramite operazioni di recovery • Azione involontaria di un utente che porta alla alterazione di dati tracciata e reversibile • Modifica di un documento non ancora validato dal proprio autore.
Divulgazione non Autorizzata	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Malfunzionamento del sistema di oscuramento del sistema dipartimentale che invia a SOLE • Consegna di un CD con dati dei pazienti ad altra struttura senza autorizzazione	• Il medico sul proprio sistema dipartimentale seleziona il paziente Mario Rossi ma visita il paziente Luca Bianchi. Inserisce anamnesi e gli altri valori di refertazione ed invia a SOLE. • Infezione virale di un PC con un virus che dalla scheda tecnica non trasmette dati su internet • Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
Accesso non Autorizzato	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi • Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema clinico	• Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi • Accesso non autorizzata di un documento non ancora validato dal proprio autore.
Indisponibilità temporanea del dato	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato.	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale	• Infezione da ransomware che comporta la temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal backup • cancellazione accidentale dei dati da parte di una persona non autorizzata • perdita della chiave di decrittografia di dati crittografati in modo sicuro • irraggiungibilità di un sito di stoccaggio delle cartelle cliniche poste in montagna per isolamento neve	• Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso

Un data breach, quindi, non è solo un attacco informatico, ma può consistere anche in un accesso abusivo, un incidente (es. un incendio o una calamità naturale), nella semplice perdita di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno), nella sottrazione di documenti con dati personali (es. furto di un notebook di un dipendente). I casi di data breach per

le casistiche già descritte si estendono ai documenti cartacei o su supporti analogici. La comunicazione involontaria di documenti, o in generale di dati, che non abbiano vero senso compiuto/riconducibilità verso l'interessato non è considerato data breach, ma è considerato un normale errore procedurale.

Questo poiché:

- Chi riceve non può sapere a quale paziente fisico è riferito il testo;
- Il paziente fisico non è danneggiato poiché nessuno riferimento alla sua persona è stato diffuso.

Notifica di una violazione dei dati personali

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

Questo servizio *online* per la notifica di una violazione dei dati personali deve essere utilizzato esclusivamente da soggetti (pubbliche amministrazioni, imprese, associazioni, partiti, professionisti, ecc.) che trattano dati personali in qualità di titolari del trattamento.

Per rivolgersi al Garante in qualità di interessato, per lamentare una violazione della disciplina in materia di protezione dei dati personali, occorre inviare una segnalazione (art. 144 del Codice in materia di protezione dei dati personali) che il Garante può valutare anche ai fini dell'emanazione di provvedimenti correttivi, oppure proporre un reclamo (art. 77 del Regolamento (UE) 2016/679 e artt. da 140-*bis* a 143 del Codice in materia di protezione dei dati personali).

Maggiori informazioni sono disponibili sul sito istituzionale del Garante (https://www.gpdp.it/web/guest/home/diritti/come-agire-per-tutelare-i-tuoi-dati-personali).

Facsimile a titolo dimostrativo non utilizzabile per l'invio della notifica al Garante.

Notifica di una violazione dei dati personali

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

A) Dati del soggetto che effettua la notifica

Il soggetto che effettua la notifica è la persona fisica che, per conto titolare del trattamento, tramite questa procedura *online* notifica una violazione dei dati personali al Garante, assumendosi la responsabilità circa la veridicità delle informazioni fornite. Pertanto, la notifica dovrà essere effettuata dal rappresentante legale del titolare del trattamento o da un altro soggetto che agisce su sua delega.

Il sottoscritto Cognome[1*] …….. Nome[1*] …….
E-mail[2*] ……
nella sua qualità[3] di

0 rappresentante legale

0 delegato del rappresentante legale

Cognome[4*] …….. Nome[4*] …….

notifica la seguente violazione di dati personali e ☐ dichiara di aver preso visione dell'informativa sul trattamento dei dati personali e di essere consapevole 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*) o dell'art. 44 del d.lgs. 51/2018 (*Falsità in atti e dichiarazioni al Garante*), salvo che il fatto non costituisca più grave reato.

———————————

[1] Indicare il **Cognome** e il **Nome** del soggetto che effettua la notifica (e che successivamente dovrà apporre la sua firma digitale, conformemente alle istruzioni che riceverà via e-mail).

[2] Indicare un indirizzo **E-mail** valido per la ricezione delle istruzioni per il completamento della procedura di notifica. Nel caso venga indicata una casella PEC, verificare che la stessa sia abilitata alla ricezione di messaggi di posta elettronica ordinaria. Si consiglia, inoltre, di verificare che il messaggio non sia stato spostato automaticamente o per errore nella cartella "spam" o "posta indesiderata.

[3] Indicare se il soggetto che effettua la notifica è il "rappresentante legale" del Titolare del trattamento dati – di cui alla successiva Sez. C - oppure se agisce in **qualità** di "delegato del rappresentante legale.

[4] Qualora la notifica venga effettuata su delega del rappresentante legale è necessario indicare il Cognome ed il Nome del soggetto delegante (il rappresentante legale).

B) Tipo di notifica

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore (**Prima notifica**). Qualora e nella misura in cui il titolare del trattamento non disponga di tutte le informazioni, può fornirle in fasi successive (**Notifica integrativa**) senza ulteriore ingiustificato ritardo (cfr. art. 33, par. 4, del Regolamento).

0 ***Prima notifica***

0 a) Completa

0 b) Preliminare[1]

La notifica viene effettuata

0 ai sensi dell'art. 33 del RGPD

0 ai sensi dell'art. 26 d.lgs. 51/2018

0 ***Notifica integrativa***[2]

0 c) fascicolo n. [3*] ..... PIN [3*] .....

———————————

[1] Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione impegnandosi ad effettuare una successiva notifica integrativa per completare il processo di notifica.

[2] Il titolare del trattamento, avvalendosi delle previsioni di cui all'art. 33 par. 4 del Regolamento, integra una precedente notifica.

[3] È necessario inserire il numero del fascicolo ed il relativo PIN. Il numero di **fascicolo** unitamente al PIN sono indicati nella e-mail, indirizzata al soggetto che ha effettuato la prima notifica, con la quale è stata comunicata la corretta conclusione della procedura.

B1) Motivo dell'integrazione

Se procedi con la notifica integrativa per i motivi a) o b) troverai le informazioni che hai già fornito con l'ultima notifica e che potrai modificare. Il suo contenuto, previa integrazione o modifica, annulla e sostituisce la precedente.

Se la notifica che intendi integrare è stata trasmessa con le precedenti modalità non troverai le informazioni che hai già fornito, e non sarà possibile compilare la sez. C e i punti 2 e 3 della sez. F. La notifica integrativa, ed il suo contenuto, integrerà e sostituirà la precedente notifica.

1. Si procede all'integrazione per:

- 0 a) Fornire ulteriori informazioni senza completare il processo di notifica
- 0 b) Fornire ulteriori informazioni e completare il processo di notifica
- 0 c) Completare il processo di notifica senza fornire ulteriori informazioni
- 0 d) Annullare una precedente notifica per le seguenti motivazioni:

C) Titolare del trattamento

1. *Il titolare del trattamento è:*

Indicare l'eventuale registro all'interno del quale è censito il Titolare/Responsabile del trattamento che effettua la comunicazione. A tal fine si rappresenta che (cfr. DL 19 ottobre 2012, n. 179) tutte le imprese costituite in forma societaria e tutte le imprese individuali iscritte al registro delle imprese o all'albo delle imprese artigiane, nonché tutti i professionisti iscritti ad Ordini o Collegi professionali sono censiti all'interno dell'Indice nazionale dei domicili digitali delle imprese e dei professionisti (INIPEC). Inoltre, tutte le pubbliche amministrazioni (es. scuole, comuni, ecc.) sono iscritte nell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA).

0 Censito nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti
(INI-PEC www.inipec.gov.it - art. 6-bis Codice Amministrazione Digitale - D.Lgs n. 82/2005)

0 Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi - *(Tipologie Enti: Pubbliche Amministrazioni)*
(*IPA www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005*)

0 Non censito in nessuno dei due precedenti indici

2. *Dati del titolare del trattamento*

Indicare le informazioni relative al Titolare del trattamento (nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).

Denominazione* .....
Codice Fiscale [1]* ..... Soggetto privo di C.F./P.IVA italiana ☐
Stato* .....
Provincia* ..... Comune* ..... CAP* .....
Indirizzo* .....
Telefono* .....
E-mail[2]* .....
PEC[2]* .....

———————————

[1] In relazione all'indicazione del Codice Fiscale si rappresenta che:

- I soggetti censiti nell'indice IPA appartenenti alla categoria "Pubbliche Amministrazioni" **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora ne siano in possesso);
- Le imprese censite nell'indice INI-PEC **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora non coincidente con il Codice Fiscale);
- I professionisti censiti nell'indice INI-PEC **devono** indicare il numero di Partita IVA utilizzato per lo svolgimento dell'attività professionale;
- Solo i soggetti stranieri o le organizzazioni prive di Codice Fiscale e P.IVA devono selezionare la casella "Soggetto Privo di CF/P.IVA".

[2] Per i soggetti che risultano essere censiti in uno degli indici INI-PEC o IPA è **obbligatorio** fornire l'indirizzo PEC, mentre il conferimento dell'indirizzo e-mail è facoltativo. Per i soggetti che non risultano essere censiti in uno dei due citati indici, o che operano in un altro Stato, è obbligatorio fornire un valido indirizzo e-mail, mentre il conferimento della PEC è facoltativo.

Notifica di una violazione dei dati personali

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

C1) Rappresentante del titolare del trattamento non stabilito nello Spazio Economico Europeo

Il titolare del trattamento non stabilito nello Spazio Economico Europeo, qualora offra beni o servizi a interessati nello Spazio Economico Europeo, oppure effettui il monitoraggio del loro comportamento (cfr. art. 3, par. 2, del Regolamento), è tenuto, ai sensi dell'art. 27 del Regolamento, a designare per iscritto un rappresentante in uno dei Paesi dello Spazio Economico Europeo in cui si trovano i predetti interessati, fatti salvi i casi in cui il trattamento è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati o dati relativi a condanne penali e reati, ed è improbabile che presenti un rischio per i diritti e le libertà degli interessati, oppure il trattamento è effettuato da autorità o organismi pubblici.

1. Rappresentante del titolare del trattamento

0 a) Compila la sezione

0 b) Procedi con la notifica senza compilare questa sezione

2. Dati del rappresentante del titolare del trattamento

Denominazione[1*] .....

Codice Fiscale/P.IVA* ..... Soggetto privo di C.F./P.IVA italiana ☐

Stato* .....

Provincia* ..... Comune* ..... CAP* .....

Indirizzo* .....

Telefono* .....

E-mail[2*] .....

PEC[2*] .....

———————————

[1] Indicare le informazioni relative al Rappresentante del titolare del trattamento (nel caso di impresa indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).

[2] È obbligatorio fornire almeno un recapito tra E-mail e PEC.

D) Dati di contatto per informazioni relative alla violazione

Il titolare del trattamento deve 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 (cfr. art. 33, par. 3, lett. b), del Regolamento).

o ***1) Responsabile della protezione dei dati***

- o i cui dati di contatto sono stati già comunicati con la comunicazione protocollo[1*] n.……..
- o i cui dati di contatto sono stati già comunicati al Garante, ma al momento non si dispone[2] del numero di protocollo della relativa comunicazione

Cognome* …… Nome* ……..
E-mail* ……..
Recapito telefonico per eventuali comunicazioni* ……

o ***2) Altro soggetto***

Cognome* …… Nome* ……..
E-mail* ……..
Recapito telefonico per eventuali comunicazioni* ……
Funzione rivestita* ……

———————————

[1] Indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD.

[2] Selezionare questa opzione se al momento della compilazione non è possibile reperire il numero di protocollo assegnato alla comunicazione dei dati di contatto che sarà comunicato con una successiva notifica integrativa.

E) Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare, responsabile[1])

Denominazione[2*] ……

Codice Fiscale[3*] ……Soggetto privo di C.F./P.IVA ☐

Ruolo O Contitolare O Responsabile

Denominazione[2*] ……

Codice Fiscale[3*] ……Soggetto privo di C.F./P.IVA ☐

Ruolo O Contitolare O Responsabile

Denominazione[2*] ……

Codice Fiscale[3*] ……Soggetto privo di C.F./P.IVA ☐

Ruolo O Contitolare O Responsabile

———————————

[1] In tale tipologia rientra anche l'altro responsabile (c.d. sub-responsabile) di cui all'art. 28, par. 2, del RGPD o all'art. 18, comma 2, del d.lgs. 51/2018.

[2] Nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale.

[3] In relazione all'indicazione del Codice Fiscale si rappresenta che:

- I soggetti censiti nell'indice IPA appartenenti alla categoria "Pubbliche Amministrazioni" **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora ne siano in possesso);
- Le imprese censite nell'indice INI-PEC **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora non coincidente con il Codice Fiscale);
- I professionisti censiti nell'indice INI-PEC **devono** indicare il numero di Partita IVA utilizzato per lo svolgimento dell'attività professionale;

  Solo i soggetti stranieri o le organizzazioni prive di Codice Fiscale e P.IVA devono selezionare la casella "Soggetto Privo di CF/P.IVA".

Notifica di una violazione dei dati personali

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

F) Informazioni sulla violazione

1. *Momento in cui è avvenuta la violazione*

- o a) Il ___ /___ /_____
- o b) Dal ___/___ /_____ (la violazione è ancora in corso)
- o c) Dal ___/___ /_____ al ___ /___ /_____
- o d) In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. *Modalità con la quale il titolare è venuto a conoscenza della violazione*

- o a) Rilevazione da parte del titolare[1]
- o b) Comunicazione da parte del responsabile del trattamento
- o c) Segnalazione da parte di un interessato
- o d) Segnalazione da parte di un soggetto esterno
- o e) Notizie stampa
- o f) Altro

3. *Momento in cui il titolare è venuto a conoscenza della violazione*

Data …… **Ora** ……..

4. *Motivi del ritardo (in caso di notifica oltre le 72 ore)*

5. *Natura della violazione*

[ ] a) Perdita di riservatezza[2]
[ ] b) Perdita di integrità[3]
[ ] c) Perdita di disponibilità[4]

6. *Causa della violazione*

[ ] a) Azione intenzionale interna
[ ] b) Azione accidentale interna
[ ] c) Azione intenzionale esterna
[ ] d) Azione accidentale esterna
[ ] e) Sconosciuta

[ ] **f)** Non ancora determinata

7. *Descrizione della violazione*[5]

8. *Descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione*

9. *Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti*

10. Categorie di interessati coinvolti nella violazione

[ ] a) Dipendenti/Consulenti
[ ] b) Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
[ ] c) Associati, soci, aderenti, simpatizzanti, sostenitori
[ ] d) Soggetti che ricoprono cariche sociali
[ ] e) Beneficiari o assistiti
[ ] f) Pazienti
[ ] g) Minori
[ ] h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
[ ] i) Altro

[ ] l) Categorie ancora non determinate

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

o a) N. …….. interessati
o b) Circa n. …….. interessati
o c) Non determinabile
o d) Non ancora determinato

12. Categorie di dati personali oggetto di violazione

[ ] a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
[ ] b) Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
[ ] c) Dati di accesso e di identificazione (username, password, customer ID, altro…)
[ ] d) Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
[ ] e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
[ ] f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
[ ] g) Dati di profilazione
[ ] h) Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
[ ] i) Dati relativi all'ubicazione
[ ] l) Dati che rivelano l'origine razziale o etnica
[ ] m) Dati che rivelano le opinioni politiche
[ ] n) Dati che rivelano le convinzioni religiose o filosofiche
[ ] o) Dati che rivelano l'appartenenza sindacale
[ ] p) Dati relativi alla vita sessuale o all'orientamento sessuale
[ ] q) Dati relativi alla salute
[ ] r) Dati genetici

[ ] s) Dati biometrici
[ ] t) Altro

[ ] u) Categorie ancora non determinate

13. *Numero (anche approssimativo) di registrazioni[6] dei dati personali oggetto di violazione*

o a) N. ……..
o b) Circa n. ……..
o c) Non determinabile
o d) Non ancora determinato

14. *Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati*

15. *Allegati*

[ ] Intendo allegare un documento contenente ulteriori informazioni

———————————

1. Es. verifiche interne, monitoraggi, ecc
2. Diffusione/ accesso non autorizzato o accidentale
3. Modifica non autorizzata o accidentale
4. Impossibilità di accesso o distruzione non autorizzata o accidentale
5. Indicare le circostanze in cui si è verificata la violazione e le cause, tecniche o organizzative, che l'hanno determinata
6. Ad esempio numero di fatture, ordini, referti, immagini, record di un database o numero di transazioni.

G) Probabili conseguenze della violazione

1. Probabili conseguenze della violazione per gli interessati

1.1. In caso di perdita di riservatezza:

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

[ ] e) In corso di valutazione[4]

1.2. In caso di perdita di integrità:

[ ] a) I dati sono stati modificati e resi inconsistenti
[ ] b) I dati sono stati modificati mantenendo la consistenza
[ ] c) Altro

[ ] d) In corso di valutazione[4]

1.3. In caso di perdita di disponibilità:

[ ] a) Mancato accesso a servizi
[ ] b) Malfunzionamento e difficoltà nell'utilizzo di servizi
[ ] c) Altro

[ ] d) In corso di valutazione[4]

1.4. Ulteriori considerazioni sulle probabili conseguenze

2. Potenziale impatto per gli interessati

[ ] a) Perdita del controllo dei dati personali
[ ] b) Limitazione dei diritti
[ ] c) Discriminazione
[ ] d) Furto o usurpazione d'identità
[ ] e) Frodi
[ ] f) Perdite finanziarie
[ ] g) Decifratura non autorizzata della pseudonimizzazione
[ ] h) Pregiudizio alla reputazione
[ ] i) Perdita di riservatezza dei dati personali protetti da segreto professionale
[ ] l) Conoscenza da parte di terzi non autorizzati
[ ] m) Qualsiasi altro danno economico o sociale significativo

[ ] n) Non ancora definito

3. Gravità del potenziale impatto per gli interessati

o a) Trascurabile
o b) Bassa
o c) Media
o d) Alta
o e) Non ancora definita

Motivazioni

4. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

H) Misure adottate a seguito della violazione

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

2. Misure tecniche e organizzative adottate (o di cui si propone l'adozione[1]) per prevenire simili violazioni future

3. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

———————————

1. Nella descrizione distinguere le misure adottate da quelle in corso di adozione

I) Valutazione del rischio per gli interessati

Non sono state fornite alcune delle informazioni (es. categorie e numero di interessati, categorie e numero di registrazioni di dati personali, probabili conseguenze della violazione, ecc.) di cui il titolare del trattamento dovrebbe tenere conto nella valutazione del rischio per i diritti e le libertà degli interessati derivante dalla violazione dei dati personali. Pertanto si invita il titolare del trattamento a prestare particolare attenzione nella compilazione della presente sezione, fornendo le motivazioni che lo hanno portato a ritenere che la violazione dei dati personali sia suscettibile, o meno, di presentare un rischio elevato per gli interessati.

Il Regolamento (spec. cons. nn. 75 e 76) suggerisce che, di norma, nella valutazione del rischio si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità dei rischi per i diritti e le libertà degli interessati e che tali rischi dovrebbero essere determinati in base a una valutazione oggettiva.
Le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018, individuano i seguenti fattori da considerare – a fronte di una violazione dei dati personali – nella valutazione del rischio per i diritti e le libertà degli interessati: il tipo di violazione; la natura, il carattere sensibile e il volume dei dati personali; la facilità di identificazione degli interessati; la gravità delle conseguenze per gli interessati; le caratteristiche particolari dell'interessato; le caratteristiche particolari del titolare del trattamento dei dati; nonché il numero di interessati coinvolti.

1. Il titolare del trattamento ritiene[1] che:

- o a) la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- o b) la violazione non sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- o c) siano necessari ulteriori elementi per effettuare la valutazione del rischio per i diritti e le libertà delle persone fisiche

Motivazioni

2. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

L) Comunicazione della violazione agli interessati

Si evidenzia che, 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 è tenuto, ai sensi dell'art. 34 del Regolamento, a comunicare la violazione agli interessati coinvolti senza ingiustificato ritardo, a meno che sia soddisfatta una delle condizioni previste dal par. 3 del citato articolo.

1. La violazione è stata comunicata direttamente agli interessati?

- o a) Sì, è stata comunicata il ___/___/_____
- o b) No, sarà comunicata entro il ___/___/_____
- o c) No, sono tuttora in corso le dovute valutazioni
- o d) No, perché la violazione non è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- o e) No e non sarà comunicata perché:

[ ] e1) il titolare 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 (es. cifratura);

Descrivere le misure applicate

[ ] e2) il titolare 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

[ ] e3) detta comunicazione richiederebbe sforzi sproporzionati. Il titolare ha proceduto o procederà con una comunicazione pubblica o una misura simile, tramite la quale gli interessati sono o saranno informati con analoga efficacia.

Descrivere la modalità tramite la quale gli interessati sono stati informati

Notifica di una violazione dei dati personali

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

2. Numero di interessati a cui è stata comunicata la violazione

N. …….. interessati

3. Canale utilizzato per la comunicazione agli interessati

[ ] a) SMS
[ ] b) Posta cartacea
[ ] c) Posta elettronica
[ ] d) Altro

4. Contenuto della comunicazione agli interessati

5. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

M) Altre informazioni

1. La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[1]?

O Sì O No

Indicare a quale organismo e in virtù di quale norma

2. È stata effettuata la segnalazione all'autorità giudiziaria o di polizia?

O Sì O No

Note

———————————

1. Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

N) Informazioni relative a violazioni transfrontaliere

Un trattamento transfrontaliero (cfr. art. 4, punto 23), del Regolamento) è un trattamento che ha luogo nell'ambito di stabilimenti in più di un Paese dello Spazio Economico Europeo (di cui fanno parte gli Stati membri dell'Unione Europea, nonché l'Islanda, il Liechtenstein e la Norvegia), oppure che ha luogo nell'ambito di un unico stabilimento in un Paese dello Spazio Economico Europeo, ma che può avere impatti significativi sui diritti e sulle libertà di interessati in più di un Paese dello Spazio Economico Europeo.

1. ***La violazione riguarda un trattamento transfrontaliero effettuato da un titolare stabilito all'interno dello Spazio Economico Europeo?***

   - o a) Sì
   - o b) No
   - o c) Sono tuttora in corso le dovute valutazioni

2. ***Indicare l'autorità di controllo capofila[1]***

   - o a) Garante per la protezione dei dati personali
   - o b) Altra autorità di controllo: [Selezionare]
   - o c) Non si dispone di elementi per individuare l'autorità di controllo capofila

3. ***Indicare i Paesi dello Spazio Economico Europeo in cui si trovano stabilimenti del titolare, specificando quelli coinvolti nella violazione, o in cui si trovano gli interessati coinvolti nella violazione***

	Stabilimenti del titolare	Stabilimenti coinvolti nella violazione	Interessati coinvolti nella violazione
Italia	[ ]	[ ]	[ ]
Austria	[ ]	[ ]	[ ]
Belgio	[ ]	[ ]	[ ]
Bulgaria	[ ]	[ ]	[ ]
Cipro	[ ]	[ ]	[ ]
Croazia	[ ]	[ ]	[ ]
Danimarca	[ ]	[ ]	[ ]
Estonia	[ ]	[ ]	[ ]
Finlandia	[ ]	[ ]	[ ]
Francia	[ ]	[ ]	[ ]
Germania	[ ]	[ ]	[ ]
Grecia	[ ]	[ ]	[ ]
Irlanda	[ ]	[ ]	[ ]
Islanda	[ ]	[ ]	[ ]
Lettonia	[ ]	[ ]	[ ]
Liechtenstein	[ ]	[ ]	[ ]
Lituania	[ ]	[ ]	[ ]

Lussemburgo	[ ]	[ ]	[ ]
Malta	[ ]	[ ]	[ ]
Norvegia	[ ]	[ ]	[ ]
Paesi Bassi	[ ]	[ ]	[ ]
Polonia	[ ]	[ ]	[ ]
Portogallo	[ ]	[ ]	[ ]
Rep. Ceca	[ ]	[ ]	[ ]
Romania	[ ]	[ ]	[ ]
Slovacchia	[ ]	[ ]	[ ]
Slovenia	[ ]	[ ]	[ ]
Spagna	[ ]	[ ]	[ ]
Svezia	[ ]	[ ]	[ ]
Ungheria	[ ]	[ ]	[ ]

4. *Indicare le altre autorità di controllo a cui è stata eventualmente notificata la violazione*

[ ] Austria - Data Protection Authority
[ ] Belgio - Data Protection Authority
[ ] Bulgaria - Commission for Personal Data Protection
[ ] Cipro - Office of the Commissioner for Personal Data Protection
[ ] Croazia - Personal Data Protection Agency - AZOP
[ ] Danimarca - Data Protection Agency
[ ] Estonia - Data Protection Inspectorate
[ ] Finlandia - Office of the Data Protection Ombudsman
[ ] Francia - CNIL - National Commission for Informatics and Liberties
[ ] Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI)
[ ] Germania (Baden-Wurttemberg) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Bavaria - Private Sector) - Bavarian Lander Office for Data Protection Supervision (BayLDA)
[ ] Germania (Bavaria - Public sector) - Lander Commissioner for Data Protection (BayLfD)
[ ] Germania (Berlin) - Berlin Commissioner for Data Protection and Freedom of Information
[ ] Germania (Brandenburg) - Lander Commissioner for Data Protection and the Right for Access to Information
[ ] Germania (Bremen) - Lander Commissioner for Data Protection and Freedom of Information - Free Hanseatic city of Bremen
[ ] Germania (Hamburg) - Hamburg Commissioner for Data Protection and Freedom of Information
[ ] Germania (Hesse) - Hessian Commissioner for Data Protection and Freedom of Information
[ ] Germania (Lower Saxony) - Lander Commissioner for Data Protection (LfD)
[ ] Germania (Mecklenburg-Western Pomerania) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (North Rhine-Westphalia) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Rhineland-Palatinate) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saarland) - Independent Data Protection Center Saarland - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saxony) - Saxon Data Protection Commissioner
[ ] Germania (Saxony-Anhalt) - Lander Commissioner for Data Protection
[ ] Germania (Thuringia) - Thuringian Lander Commissioner for Data Protection and Freedom of Information (TLfDI)
[ ] Grecia - Hellenic Data Protection Authority
[ ] Irlanda - Data Protection Commission (DPC)

[ ] Islanda - Data Protection Authority
[ ] Lettonia - Data State Inspectorate
[ ] Liechtenstein - Data Protection Authority
[ ] Lituania - State Data Protection Inspectorate
[ ] Lituania - The Office of Inspector of Journalist Ethics
[ ] Lussemburgo - National Commission for Data Protection (CNPD)
[ ] Malta - Office of the Information and Data Protection Commissioner
[ ] Norvegia - Norwegian Data Protection Authority
[ ] Paesi Bassi - Authority for Personal Data
[ ] Polonia - Office for the Protection of Personal Data
[ ] Portogallo - National Commission for Data Protection (CNPD)
[ ] Rep. Ceca - Office for Personal Data Protection
[ ] Romania - National Supervisory Authority For Personal Data Processing
[ ] Slovacchia - Office for Personal Data Protection
[ ] Slovenia - Information Commissioner
[ ] Spagna - Spanish Agency for Data Protection
[ ] Svezia - Data Protection Authority
[ ] Ungheria - National Authority for Data Protection and Freedom of Information

[ ] Intendo allegare copia (in lingua inglese) della notifica effettuata

———————————

1. L'autorità di controllo dello stabilimento principale in cui ha luogo il trattamento o dello stabilimento unico del titolare del trattamento

O) Informazioni relative a violazioni che riguardano trattamento effettuato da un titolare stabilito al di fuori dello Spazio Economico Europeo

Il Regolamento si applica anche al trattamento di dati personali di interessati che si trovano nello Spazio Economico Europeo, effettuato da un titolare del trattamento che non è stabilito nello Spazio Economico Europeo, laddove tale trattamento riguardi: a) l'offerta di beni o la fornitura di servizi a interessati nello Spazio Economico Europeo, oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dello Spazio Economico Europeo (cfr. art. 3, par. 2, del Regolamento)

1. ***La violazione riguarda un trattamento, a cui si applica il Regolamento, effettuato da un titolare stabilito al di fuori dello Spazio Economico Europeo?***

   o a) Sì
   o b) No

2. ***Indicare gli altri Paesi dello Spazio Economico Europeo in cui si trovano gli interessati coinvolti nella violazione***

   [ ] Austria
   [ ] Belgio
   [ ] Bulgaria
   [ ] Cipro
   [ ] Croazia
   [ ] Danimarca
   [ ] Estonia
   [ ] Finlandia
   [ ] Francia
   [ ] Germania
   [ ] Grecia
   [ ] Irlanda
   [ ] Islanda
   [ ] Lettonia
   [ ] Liechtenstein
   [ ] Lituania
   [ ] Lussemburgo
   [ ] Malta
   [ ] Norvegia
   [ ] Paesi Bassi
   [ ] Polonia
   [ ] Portogallo
   [ ] Rep. Ceca
   [ ] Romania
   [ ] Slovacchia
   [ ] Slovenia
   [ ] Spagna

[ ] Svezia
[ ] Ungheria

3. *Indicare le altre autorità di controllo a cui è stata eventualmente notificata la violazione*

[ ] Austria - Data Protection Authority
[ ] Belgio - Data Protection Authority
[ ] Bulgaria - Commission for Personal Data Protection
[ ] Cipro - Office of the Commissioner for Personal Data Protection
[ ] Croazia - Personal Data Protection Agency - AZOP
[ ] Danimarca - Data Protection Agency
[ ] Estonia - Data Protection Inspectorate
[ ] Finlandia - Office of the Data Protection Ombudsman
[ ] Francia - CNIL - National Commission for Informatics and Liberties
[ ] Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI)
[ ] Germania (Baden-Wurttemberg) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Bavaria - Private Sector) - Bavarian Lander Office for Data Protection Supervision (BayLDA)
[ ] Germania (Bavaria - Public sector) - Lander Commissioner for Data Protection (BayLfD)
[ ] Germania (Berlin) - Berlin Commissioner for Data Protection and Freedom of Information
[ ] Germania (Brandenburg) - Lander Commissioner for Data Protection and the Right for Access to Information
[ ] Germania (Bremen) - Lander Commissioner for Data Protection and Freedom of Information - Free Hanseatic city of Bremen
[ ] Germania (Hamburg) - Hamburg Commissioner for Data Protection and Freedom of Information
[ ] Germania (Hesse) - Hessian Commissioner for Data Protection and Freedom of Information
[ ] Germania (Lower Saxony) - Lander Commissioner for Data Protection (LfD)
[ ] Germania (Mecklenburg-Western Pomerania) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (North Rhine-Westphalia) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Rhineland-Palatinate) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saarland) - Independent Data Protection Center Saarland - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saxony) - Saxon Data Protection Commissioner
[ ] Germania (Saxony-Anhalt) - Lander Commissioner for Data Protection
[ ] Germania (Thuringia) - Thuringian Lander Commissioner for Data Protection and Freedom of Information (TLfDI)
[ ] Grecia - Hellenic Data Protection Authority
[ ] Irlanda - Data Protection Commission (DPC)
[ ] Islanda - Data Protection Authority
[ ] Lettonia - Data State Inspectorate
[ ] Liechtenstein - Data Protection Authority
[ ] Lituania - State Data Protection Inspectorate
[ ] Lituania - The Office of Inspector of Journalist Ethics
[ ] Lussemburgo - National Commission for Data Protection (CNPD)
[ ] Malta - Office of the Information and Data Protection Commissioner
[ ] Norvegia - Norwegian Data Protection Authority
[ ] Paesi Bassi - Authority for Personal Data
[ ] Polonia - Office for the Protection of Personal Data
[ ] Portogallo - National Commission for Data Protection (CNPD)
[ ] Rep. Ceca - Office for Personal Data Protection
[ ] Romania - National Supervisory Authority For Personal Data Processing
[ ] Slovacchia - Office for Personal Data Protection
[ ] Slovenia - Information Commissioner

[ ] Spagna - Spanish Agency for Data Protection
[ ] Svezia - Data Protection Authority
[ ] Ungheria - National Authority for Data Protection and Freedom of Information

[ ] Intendo allegare copia (in lingua inglese) della notifica effettuata