DELIBERAZIONE DEL DIRETTORE GENERALE n. 525 del 28 SET. 2023

OGGETTO: Approvazione della Procedura aziendale per la gestione delle violazioni dei dati personali (data breach)

DELIBERAZIONE ADOTTATA DAL DIRETTORE GENERALE DOTT.SSA PAOLA LATTUADA

SU PROPOSTA DEL REFERENTE AZIENDALE PRIVACY

accertata la competenza procedurale, sottopone in data 28 SET. 2023 l'allegata proposta di deliberazione sull'argomento all'oggetto specificato, il cui onere rientra nel budget assegnato.

Il Responsabile del Procedimento
Referente aziendale Privacy
Avv. Sarah Avietti

ATTESTAZIONE COPERTURA ECONOMICA

Si attesta la regolarità contabile, la copertura economica e l'imputazione a bilancio degli oneri/introiti derivanti dal presente provvedimento con annotazione:

- Il presente provvedimento non comporta oneri diretti a carico del bilancio aziendale.

Il Direttore UOC Bilancio, Programmazione Finanziaria e Contabilità
Dott.ssa Emilia Martignoni

DELIBERAZIONE DEL DIRETTORE GENERALE n. 525 del 28 SET. 2023

IL DIRETTORE GENERALE

Viste:
- la DGR n. X/4475 del 10/12/2015 di costituzione, a partire dal 01/01/2016, dell'Azienda Socio Sanitaria Territoriale (ASST) Centro Specialistico Ortopedico Traumatologico Gaetano Pini/CTO;
- la DGR XI/4538 del 15/04/2021 di nomina della Dott.ssa Paola Lattuada quale Direttore Generale dell'Azienda Socio Sanitaria Territoriale (ASST) Gaetano Pini-CTO per il periodo 19/04/2021 - 18/04/2024;
- la deliberazione aziendale n. 240 del 19/04/2021 di presa d'atto della predetta DGR XI/4538/2021 e di insediamento dal 19/04/2021 sino al 18/04/2024 della Dott.ssa Paola Lattuada quale Direttore Generale dell'ASST G. Pini-CTO;

Richiamati:
- il Regolamento (UE) 2016/679 relativo alla Protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (in seguito "GDPR", General Data Protection Regulation), applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018, che nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato principalmente sulla valutazione dei rischi per i diritti e le libertà degli interessati, attribuisce ai Titolari del trattamento il compito di assicurare e di comprovare il rispetto dei principi applicabili al trattamento dei dati personali e di adottare le misure ritenute più idonee ed opportune (c.d. principio di responsabilizzazione o accountability);
- il Decreto Legislativo n.101 del 10 agosto 2018, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo, in attuazione dell'art.13 della legge di delega europea 2016-2017 (legge 25 ottobre 2017, n.163), che ha introdotto disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR, novellando il codice della privacy di cui al D.Lgs. n.196/2003;
- la deliberazione aziendale n. 170 del 25/03/2021, con cui l'ASST G. Pini-CTO ha approvato l'assetto organizzativo interno in attuazione del Regolamento UE 2016/679 in materia di protezione dei dati personali;

Rilevato che:
- il GDPR prevede tra gli elementi caratterizzanti e innovativi il "principio di responsabilizzazione" (c.d. accountability), ponendo al centro del nuovo quadro normativo nuovi adempimenti, tra cui quelli previsti dagli artt. 33 e 34 del Regolamento UE e in particolare quello relativo all'adozione di una specifica procedura di gestione delle violazioni dei dati personali (Data Breach);
- per "violazione dei dati personali" si intende, ai sensi dell'art. 4 comma 12, "*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*";
- l'art.33 del Regolamento suddetto recita: "*nel 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*";

DELIBERAZIONE DEL DIRETTORE GENERALE n. 525 del 28 SET. 2023

- ai sensi dell'art.34 del Regolamento suddetto "*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*";

Ritenuto, in adesione al vigente dettato normativo, di adottare specifica regolamentazione volta a definire una procedura interna idonea a garantire l'efficacia, la tempestività e l'uniformità delle attività di rilevazione e segnalazione alle competenti autorità delle operazioni sospette di riciclaggio e di finanziamento al terrorismo, attraverso l'adozione di una procedura operativa aziendale;

Visto il testo della procedura aziendale per la gestione di violazione dei dati personali (data breach), allegata al presente provvedimento quale parte integrante e sostanziale, nel quale risultano declinate responsabilità e procedure attuative per l'emersione e la gestione di eventuali data breach, nonché definito il flusso degli adempimenti in caso di presunta o accertata violazione di dati personali degli incidenti di sicurezza, secondo le seguenti fasi:

A) rilevazione della violazione dei dati personali e raccolta informazioni;
B) comunicazione della violazione all'ufficio privacy aziendale – istruttoria e analisi tecnica dell'evento;
C) notifica all'autorità garante;
D) comunicazione agli interessati dove necessario;
E) altre segnalazioni dovute;
F) adozione azioni correttive/preventive;

Dato atto che la predisposizione della procedura in oggetto è stata condivisa con il Data Protection Officer (DPO) dell'azienda sanitaria, L&T Advisors - LTA S.r.l. (nominato con deliberazione n. 398/2022);

Rilevato che il presente provvedimento non comporta oneri diretti a carico del bilancio aziendale;

Ritenuto per quanto precede di approvare la procedura aziendale per la gestione di violazioni dei dati personali (data breach), demandandone il coordinamento e l'attuazione all'Ufficio Privacy e al Referente aziendale Privacy, anche ai fini della tenuta del registro aziendale degli incidenti di sicurezza e della predisposizione di iniziative informative e formative rivolte al personale aziendale;

Viste:
- l'attestazione di regolarità dell'istruttoria e legittimità del presente provvedimento espressa dal Responsabile dell'UOC proponente;
- l'attestazione di regolarità contabile e della relativa copertura economica da parte del Responsabile dell'UOC Bilancio, Programmazione finanziaria e Contabilità;

Visti i pareri del Direttore Amministrativo, del Direttore Sanitario e del Direttore Socio Sanitario, resi per quanto di competenza, ai sensi dell'art. 3 del D.Lgs. n. 502/1992 e s.m.i.;

DELIBERA

per i motivi di cui in premessa che qui si intendono integralmente trascritti

1. di approvare e adottare la Procedura aziendale per la gestione di violazioni dei dati personali (data breach), unita al presente atto quale parte integrante e sostanziale sotto la voce di

DELIBERAZIONE DEL DIRETTORE GENERALE n. 525 del 28 SET. 2023

allegato A) comprensiva dei sub-allegati 1) 2) e 3);

2. di demandare il coordinamento e l'attuazione della succitata procedura all'Ufficio Privacy e al Referente aziendale Privacy, anche ai fini della tenuta del registro aziendale degli incidenti di sicurezza e della predisposizione di iniziative informative e formative rivolte al personale aziendale;

3. di dare atto che il presente provvedimento non comporta oneri diretti a carico del bilancio aziendale;

4. di dare atto che il presente provvedimento è immediatamente esecutivo ai sensi dell'art. 17, comma 6, della L.R. n. 33/2009, così come sostituito dall'art. 1, comma 1, lett. w) della L.R. n. 23/2015;

5. di disporre la pubblicazione del presente provvedimento all'Albo Pretorio on line aziendale, ai sensi dell'articolo 17, comma 6, della L.R. n. 33/2009, così come sostituito dall'art. 1, comma 1, lett. w) della L.R. n. 23/2015.

IL DIRETTORE SANITARIO
(Dott.ssa Paola GIULIANI)

IL DIRETTORE SOCIO SANITARIO
(Dott.ssa Anna Maria MAESTRONI)

IL DIRETTORE AMMINISTRATIVO
(Dott. Luca Marcello MANGANARO)

IL DIRETTORE GENERALE
(Dott.ssa Paola LATTUADA)

Ufficio Privacy
Si attesta la regolarità amministrativa e tecnica del presente provvedimento
Responsabile del Procedimento ai sensi della L. 241/90: avv. Sarah Avietti - UOC Affari Generali e Legali
Pratica trattata da: dott.ssa Barbara Savy
(Atti Privacy n. 2023 – 01)

DELIBERAZIONE DEL DIRETTORE GENERALE n. 525 del 28 SET. 2023

RELATA DI PUBBLICAZIONE

Si certifica che la presente deliberazione è pubblicata all'albo pretorio informatico di quest'Azienda sul sito internet istituzionale, così come previsto dall'art. 32, comma 1, L. 69/2009, e dall'art. 8 del D. Lgs.33/2013, dal 29 SET. 2023 e vi rimarrà per quindici giorni consecutivi.

La deliberazione si compone di n. 5 pagine e n. 1 allegato.

UOC Affari Generali e Legali
Il Funzionario addetto

Per copia conforme all'originale per uso amministrativo
Milano, lì _____

UOC Affari Generali e Legali
Il Funzionario addetto

INDICE

1. SCOPO 2
2. CAMPO DI APPLICAZIONE 2
3. ELENCO ACRONIMI 2
4. DIAGRAMMA DI FLUSSO 3
5. MATRICE DELLE RESPONSABILITA' 3
6. DESCRIZIONE DELLE ATTIVITÀ 4
6.1 DEFINIZIONI 4
6.2 SCENARI PER I QUALI ATTIVARE LA PROCEDURA DI DATA BREACH 6
6.3 PROCEDURA DI GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI – SEGNALAZIONE INTERNA 7
6.4 PROCEDURA DI GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI – RESPONSABILI ESTERNI DEL TRATTAMENTO (RINVIO) 11
7. INDICATORI DI QUALITÀ 11
8. MODULISTICA COLLEGATA 11
9. RIFERIMENTI 12
10. ENTRATA IN VIGORE 12

	Autore	Motivo	Versione n°	Data
Revisione				
Revisione				
Revisione				
Revisione				
Revisione				

1. SCOPO

Per data breach, in italiano "violazione dei dati personali", si intende una violazione di sicurezza che comporta accidentalmente o illecitamente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Una violazione dei dati personali può scaturire sia dall'interno che dall'esterno dell'Azienda e, qualora non affrontata tempestivamente e in maniera adeguata, può comportare pericoli significativi per la privacy degli interessati cui i dati si riferiscono (es. discriminazioni, furti di identità, perdite economiche, pregiudizi alla reputazione, etc).

Il Regolamento Europeo prevede che, in caso di violazione dei dati personali, il Titolare del trattamento debba notificare 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.

La presente procedura ha l'obiettivo di gestire il flusso di attività da porre in essere nel momento in cui si sviluppi una violazione di dati personali ai sensi degli articoli 33 e 34 del Regolamento 679/2016/UE (RGPD o GDPR in lingua inglese).

La procedura coinvolge le diverse Unità Organizzative che segnaleranno l'avvenuta violazione, la funzione interna competente in materia di protezione dei dati (Ufficio Privacy) ed il Data Protection Officer (DPO).

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata osservanza di quanto in essa previsto potrà comportare l'adozione di provvedimenti Disciplinari, ovvero giusta causa di risoluzione dei contratti in essere

2. CAMPO DI APPLICAZIONE

Le istruzioni aziendali si applicano in caso di violazione dei dati personali, siano essi in formato elettronico, cartaceo, o di altra tipologia, che sono oggetto di trattamento da parte dell'ASST G.PINI-CTO.

La presente procedura si applica a tutto il personale delle Strutture dell'Azienda che, a qualsiasi titolo (dipendenti, universitari, borsisti, tirocinanti, ecc.) e in qualsiasi modalità (automatizzata, manuale, digitale, cartacea), trattano dati all'interno dell'Azienda.

3. ELENCO ACRONIMI

Sigla	Descrizione
DPO	Data Protection Officer
GDPR	General Data Protection Regulation – Regolamento 679/2016/UE
PC	Personal Computer
SIA	Sistemi Informativi Aziendali
UO	Unità Operativa
UOC	Unità Operativa Complessa

4. DIAGRAMMA DI FLUSSO

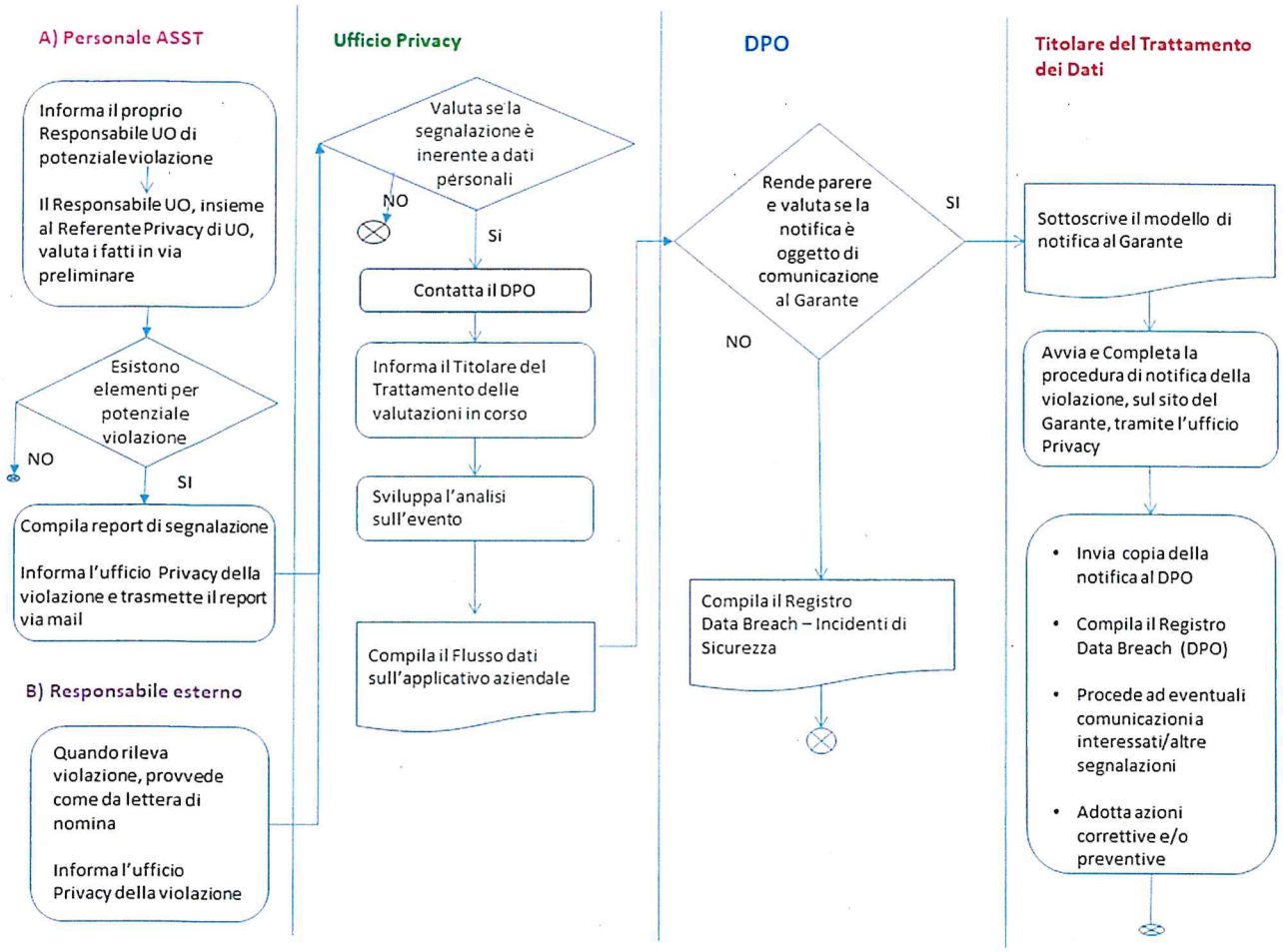

Fig. 1 Processo di gestione di potenziale data breach

5. MATRICE DELLE RESPONSABILITA'

Funzione	Responsabilità
Personale aziendale	Informa il proprio responsabile UO in relazione ad ogni potenziale violazione dati
Responsabile UO	Valuta in prima istanza la segnalazione di potenziale violazione dei dati personali. Se sussistono gli elementi per un potenziale data breach, invia il report di comunicazione interna di data breach all'ufficio Privacy
Referente Privacy di Unità Operativa	Supporta il Responsabile UO nella valutazione preliminare di segnalazioni di potenziale violazione dei dati personali.
Ufficio Privacy	Effettua l'analisi del potenziale data breach con il supporto del DPO. Supporta il Titolare del Trattamento per le azione di notifica all'Autorità Garante
DPO	Analizza l'evento di un potenziale data breach. Valuta se la segnalazione sia oggetto di notifica all'Autorità Garante. Fornisce parere al Titolare del Trattamento sull'opportunità di una notifica al Garante
Titolare del Trattamento	Sottoscrive notifica al Garante. Dà seguito ad azioni correttive/preventive

6. DESCRIZIONE DELLE ATTIVITÀ

6.1 DEFINIZIONI

Dato Personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

Dati biometrici: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Responsabile esterno del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Incaricato del trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del Titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali;

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche

che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

Interessato al trattamento: è la persona fisica identificata o identificabile a cui si riferiscono i dati personali. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, i dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Data Protection Officer (DPO) o Responsabile della Protezione dei Dati (RPD): è il soggetto designato dal titolare per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR (art. 37). Figura obbligatoria per le Pubbliche

Amministrazioni, deve essere informato tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali (art.38 del GDPR) ed è incaricato tra i suoi compiti, (art.39 del GDPR) di:
a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 GDPR;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

6.2 SCENARI PER I QUALI ATTIVARE LA PROCEDURA DI DATA BREACH

Per Data Breach si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali".
Nello specifico, l'articolo 4, p. 12 GDPR definisce la violazione dei dati personali come 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 in materia di notifica delle violazioni di dati personali (Data Breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679, precisano che le violazioni possono essere classificate in base ai seguenti tre principi 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.

Tipologia di violazione	Evento/minaccia
Violazione della riservatezza	Accesso a dati personali non autorizzato/accidentale
	Divulgazione dati personali non autorizzata/accidentale
Violazione dell'integrità	Modifica non autorizzata o accidentale di dati personali
Violazione della disponibilità	Perdita/accesso/distruzione accidentale o non autorizzata di dati personali

La procedura di data breach si applica ad ogni episodio, in cui dati personali per motivi accidentali o volontari, siano stati divulgati al di fuori delle finalità per le quali i dati erano stati raccolti.
Scenari, per i quali sarà necessario applicare la procedura di data breach, possono essere, a titolo esemplificativo e non esaustivo:

- Sottrazione di credenziali di autenticazione;
- Furto/smarrimento di PC, Notebook, Tablet, Smartphone contenenti dati personali;
- Erronea diffusione, pubblicazione o comunicazione di dati personali;
- Intrusione non autorizzata in locali in cui sono conservati/archiviati dati personali;
- Furto di archivi cartacei e/o digitali;
- Accesso non autorizzato nel sistema informativo;
- Azione di malware (virus, etc.) che siano riusciti ad eludere le misure di sicurezza aziendali;
- Smarrimento di dati personali (archiviati su supporti cartacei e digitali);
- Distruzione di dati personali (archiviati su supporti cartacei e digitali).
  A seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.
  L'articolo 32 del GDPR dispone che il Titolare del trattamento, nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, deve tenere conto, tra le altre cose, "della pseudonimizzazione e la cifratura dei dati personali", "della capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento", "della capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico", "di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

In caso di violazione dei dati personali, il Titolare del Trattamento deve, ex art. 33 del GDPR, notificare all'autorità di controllo (Garante) la violazione senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, ma soltanto se ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà delle persone fisiche.
Il criterio dirimente per valutare la necessità di avviare una procedura di notifica è pertanto la probabilità che la violazione possa porre a rischio (per la notifica all'Autorità), o a elevato rischio (per la comunicazione agli interessati) le libertà e i diritti degli individui.

6.3 PROCEDURA DI GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI – SEGNALAZIONE INTERNA

Poiché il Titolare del trattamento deve notificare senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, la violazione al Garante per la protezione dei dati personali (a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche), nel caso in cui un soggetto venga a conoscenza di una concreta, potenziale o sospetta violazione di dati personali, dovrà attivare il flusso di adempimenti di seguito descritti e schematizzati:

A) RILEVAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI E RACCOLTA INFORMAZIONI:

Tutto il personale (dipendente e collaboratore), qualora venga a conoscenza di un potenziale/sospetto/concreto data breach, anche tramite segnalazioni esterne dei cittadini/utenti, deve informare immediatamente il Responsabile di Unità Operativa o chi ne fa le veci, in caso di assenza del Responsabile. Il Responsabile dell'Unità Operativa, di concerto con il referente privacy della UO, valuta la segnalazione ricevuta. Nel caso non ci siano elementi che possano ricondurre a una potenziale violazione, la segnalazione viene archiviata. Ove, ad avviso del Responsabile UO, sussistano elementi significativi per un potenziale data breach, viene effettuata una istruttoria sommaria sulla segnalazione ricevuta, raccogliendo i dati preliminari utili all'inquadramento del caso e mettendo in atto le prime azioni per il contenimento/annullamento del danno.

Il Responsabile UO/referente privacy di UO dà una prima immediata comunicazione telefonica all'Ufficio Privacy; indicativamente entro le successive 8 ore, il dirigente/referente privacy di UO deve comunicare l'esito della Istruttoria con una breve relazione, compilando il modulo "Report per la comunicazione interna di Data Breach" - Allegato 1.

Modulo e relativa documentazione devono essere trasmessi all'ufficio Privacy, inviando una e-mail avente ad oggetto "Valutazione Violazione di sicurezza" al seguente indirizzo di posta elettronica: privacy@asst-pini-cto.it. In caso di indisponibilità della posta elettronica potranno essere recapitati all'Ufficio Privacy a mano in forma cartacea.

Indicativamente entro 12 ore dal ricevimento della Segnalazione, l'Ufficio Privacy segnala l'evento al DPO inviando una e-mail avente ad oggetto "Violazione di sicurezza" al seguente indirizzo di posta elettronica: consulenza@ltadvisors.it.

B) COMUNICAZIONE DELLA VIOLAZIONE ALL'UFFICIO PRIVACY AZIENDALE – ISTRUTTORIA E ANALISI TECNICA DELL'EVENTO

L'Ufficio Privacy, avvalendosi del supporto del DPO (per quanto di sua competenza), effettua l'analisi dell'evento sulla base delle informazioni raccolte nel modulo allegato A, e, sulla scorta dei dati disponibili, procede a:

- identificare la causa, l'entità e la natura della violazione dei dati personali; la tipologia di dati personali e le informazioni coinvolte;
- identificare la natura, la categoria e il numero di persone coinvolte (ad es. dipendenti, collaboratori, pazienti, ospiti, soggetti esterni);
- verificare se i dati e le informazioni personali non siano più disponibili ovvero se siano ancora accessibili e utilizzabili;
- determinare se la Violazione sia stata intenzionale o accidentale;
- valutare se la Violazione possa causare danni agli Interessati e determinare le probabilità e gravità del danno;
- individuare misure che permettano di ridurre o eliminare il rischio.

Il dirigente/referente privacy di UO deve adottare misure immediate per evitare ulteriori danni a seguito delle Violazioni di Sicurezza (es., solo a titolo esemplificativo, limitare l'accesso ad aree, documenti o sistemi informatici).

Il DPO e l'ufficio Privacy coinvolgono le unità operative interessate nello specifico episodio, per poter completare gli approfondimenti necessari per la valutazione dell'accaduto e raccogliere le informazioni previste nel modulo per la notifica al Garante.

Se la violazione riguarda un asset tecnologico-informatico, è previsto il coinvolgimento dell'UOC SIA e del/i amministratore/i di sistema, al fine di valutare la portata della violazione e descrivere dettagliatamente l'accaduto.

L'Ufficio Privacy redige un report dell'evento, secondo lo schema – adattabile – dell'Allegato 2, e provvede alla compilazione del flusso di data breach sull'applicativo informativo in uso in azienda.

Una volta raccolti gli elementi, nel rispetto dei termini temporali raccolti previsti dalla normativa, a conclusione dell'istruttoria, il DPO fornisce al Titolare, per il tramite dell'ufficio Privacy, il proprio parere per un'eventuale comunicazione al Garante per la protezione dei dati personali.
La valutazione può concludersi:

- con esito negativo: il DPO valuta l'episodio come NON integrante violazione dei dati personali. Se confermato dal Titolare del trattamento, l'episodio è tracciato nel registro aziendale e l'Ufficio Privacy comunica la chiusura dell'episodio senza notifica all'Autorità Garante.
- con esito positivo: il DPO valuta l'episodio come integrante violazione dei dati personali. Se confermato dal Titolare del trattamento, l'episodio è tracciato nel registro aziendale e l'Ufficio Privacy genera il fac simile di segnalazione di data breach da inviare all'Autorità Garante (successivo punto C).
- con esito positivo con onere di informativa agli interessati (successivo punto E).

Si precisa che l'art. 33 paragrafo 4, GDPR recita "Qualora nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo". Quindi è possibile effettuare la notifica per fasi nel caso in cui non si possiedono di tutti gli elementi necessari ad una notifica completa.

L'art. 33 paragrafo 1 chiarisce che non vi è obbligo di notifica della violazione quando è "improbabile" che questa comporti un rischio per i diritti e le libertà delle persone fisiche. Ne consegue che il giudizio che determina l'improbabilità del rischio deve essere riportato nel Registro delle violazioni.
Il Titolare assume le proprie determinazioni, disponendo o meno la necessità di notifica. In ogni caso, al di là delle valutazioni espresse dal DPO, la decisione finale rispetto all'accaduto è rimessa al Titolare.

C) NOTIFICA ALL'AUTORITÀ GARANTE:

Terminato il processo di valutazione, se si ritiene che vi sia stata una violazione di dati personali e se vi è una ragionevole certezza che essa presenti un rischio per i diritti e le libertà delle persone fisiche, il Titolare procede alla notifica di data breach all'Autorità Garante, nel caso in cui la violazione comporti 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 viene notificata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/.
L'avvenuta notificazione al Garante viene documentata dall'Ufficio Privacy nel Registro aziendale delle violazioni.

Nel caso in cui si sia valutato di non effettuare comunicazione all'Autorità Garante, l'evento viene in ogni caso registrato nell'applicativo informatico aziendale, nell'apposito registro degli incidenti.

La notifica deve avvenire senza ingiustificato ritardo, entro i termini previsti per norma (72 ore), decorrenti dal momento in cui i soggetti designati, autorizzati, i Responsabili sono "ragionevolmente" certi che si sia verificato un incidente di sicurezza che ha comportato una compromissione di dati".

La notifica effettuata oltre i termini di norma deve essere accompagnata dei motivi del ritardo.

D) COMUNICAZIONE AGLI INTERESSATI DOVE NECESSARIO:
Se la violazione comporta un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento provvede, senza ingiustificato ritardo, ad 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 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;
- la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misurazione simile, tramite la quale gli interessati sono informati con analoga efficacia.

Ai sensi dell'art. 34 la notifica deve almeno:

- 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;
- descrivere le probabili conseguenze della violazione dei dati personali;
- 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.

Pertanto, a valle della decisione di notificare all'Autorità Garante, l'Ufficio Privacy, avvalendosi del supporto del DPO, valuta se sussistono gli estremi per l'informazione anche agli interessati e la modalità di comunicazione decisa dal Titolare viene curata dall'Ufficio Privacy di concerto con il DPO.

E) ALTRE SEGNALAZIONI DOVUTE:

L'ufficio Privacy, a seconda dei casi specifici, verifica la necessità di informare altri organi, consultandosi con gli Uffici aziendali competenti, segnalandone i presupposti al Titolare, quali:

- CERT-PA (in caso di incidenti informatici ai sensi della Circolare AGID n. 2/2017 del 18-04-2017);
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti);
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche);
- Gestore di Identità Digitale e AGID nel caso in cui si individui un uso anomalo di un'identità SPID (Sistema Pubblico di Identità Digitale);
- Autorità Competente NIS, nel caso di incidente rilevante ex art. 12 c. 5 del D.Lgs. 65/2018.

F) AZIONI CORRETTIVE/PREVENTIVE SPECIFICHE:

Il Titolare, sulla base dell'analisi delle violazioni riportate nel Registro delle violazioni, documenta una serie di azioni di miglioramento che a titolo esemplificativo e non tassativo, si riporta di seguito:

- Individuazione di verifiche e audit mirati alla riduzione delle probabilità di violazione;
- Revisione del Sistema di Gestione della Privacy (organigramma privacy);
- Revisione delle relazioni con Clienti e Fornitori (nomina Responsabile del trattamento);
- Revisione annuale della procedura di gestione delle violazioni;
- Adozione di misure organizzative correttive e preventive, a seconda del caso specifico;
- Programmazione azioni formative/informative rivolte ai dipendenti.

6.4 PROCEDURA DI GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI – RESPONSABILI ESTERNI DEL TRATTAMENTO (RINVIO)

Ogni qualvolta l'Azienda si trovi ad affidare il trattamento di dati ad un Responsabile esterno del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati personali.

Il Responsabile Esterno del trattamento, qualora venga a conoscenza di un potenziale caso di Data Breach, deve avvisare, senza ingiustificato ritardo e nel rispetto dei tempi previsti dall'atto di nomina/accordo/convenzione/contratto, il Titolare del Trattamento.

7. INDICATORI DI QUALITÀ

Codice Indicatore	Descrizione
IND_01	Numero di segnalazioni trimestrali inviate al DPO, non trasmesse al Garante
IND_02	Numero di segnalazioni trimestrali inviate al DPO, trasmesse al Garante

8. MODULISTICA COLLEGATA

- P19_A0953_PA004MOD001 – "Report per la comunicazione interna di data breach"
- P19_A0953_PA004MOD002 – "Report di segnalazione di ipotesi di data breach"

- Autorità Garante per la Protezione dei dati personali – "Notifica di violazione dei dati personali – Facsimile"

9. RIFERIMENTI

- Regolamento (UE) 2016/679 del Parlamento Europeo del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in particolare gli articoli 33 (Notifica all'Autorità di Controllo), 34 (notifica agli interessati) e 28 (Responsabile del trattamento).
- Decreto Legislativo 10 agosto 2018 n, 101 "Disposizioni per l'adeguamento della Normativa Nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)".
- D.Lgs. 196/2003 Codice per la protezione dei dati personali.
- Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679.
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015.
- D.Lgs. 82/2005 Codice dell'Amministrazione Digitale (CAD);
- artt. 331 e 361 del Codice di Procedura Penale (obbligo di denuncia da parte del pubblico ufficiale).
- Decreto 9 gennaio 2008 del ministero degli interni in attuazione della Legge 155/2005 sulle infrastrutture critiche.
- Decreto del Presidente del Consiglio dei Ministri 1 aprile 2008 "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività" previste dall'articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale».
- Provvedimento n.209 del 27/05/2021 del Garante per la Protezione dei Dati Personali "Procedura telematica per la notifica di violazioni di dati personali (data breach)".

10. ENTRATA IN VIGORE

La presente procedura entra in vigore dalla data di adozione del relativo provvedimento di approvazione. La presente procedura sostituisce ogni precedente istruzione operativa o prassi aziendale precedentemente in uso.
Per quanto non previsto dalla presente Procedura e/o divenuto successivamente incompatibile, si applicano le disposizioni di legge e regolamentari vigenti.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

V.2021-04

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

- o rappresentante legale
- o 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).

Notifica di una violazione dei dati personali

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

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).

- o ***Prima notifica***
  - o a) Completa
  - o b) Preliminare[1]

  La notifica viene effettuata
  - o ai sensi dell'art. 33 del RGPD
  - o ai sensi dell'art. 26 d.lgs. 51/2018
- o ***Notifica integrativa***[2]
  - o 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.

Notifica di una violazione dei dati personali

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

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:

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

Notifica di una violazione dei dati personali

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

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).

- o 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)*
- o 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*)
- o 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*

- o a) Compila la sezione
- o 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).

- ***1) Responsabile della protezione dei dati***
  - i cui dati di contatto sono stati già comunicati con la comunicazione protocollo[1]* n.....
  - 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* .....

- ***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*

- a) Il ___ /___ /_____
- b) Dal ___/___ /_____ (la violazione è ancora in corso)
- c) Dal ___/___ /_____ al ___ /___ /_____
- 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*

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

- a) N. ..... interessati
- b) Circa n. ..... interessati
- c) Non determinabile
- 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*

- a) N. .....
- b) Circa n. .....
- c) Non determinabile
- 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

- a) Trascurabile
- b) Bassa
- c) Media
- d) Alta
- 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

Notifica di una violazione dei dati personali

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

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?

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

Notifica di una violazione dei dati personali

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

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

Notifica di una violazione dei dati personali

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

[ ] 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