



**Procedura di
Gestione e Notifica Data Breach
Azienda ULSS 3**

In conformità alle Linee Guida di Azienda Zero (prot. 16336/2018)



INDICE

1. Introduzione e ambito di applicazione
2. Riferimenti normativi
3. Definizioni
4. Destinatari
5. Ruoli e responsabilità
6. Attività operative
7. Rilevazione / Valutazione del *Data Breach*
8. Gestione del *Data Breach*
9. Notifica al Garante per la protezione dei dati personali
10. Comunicazione agli Interessati
11. Pianificazione degli audit
12. Archiviazione
13. Modulistica allegata alla procedura
14. Modifiche al presente documento

1. Introduzione e ambito di applicazione

Le disposizioni applicative del Regolamento UE 279/2016 adottate dall'Azienda Ulss 3 con delibera 1017/2018 prevedono, al punto 6, le disposizioni di gestione del data Breach.

La presente procedura è volta, pertanto, a declinare con maggiore dettaglio l'iter, anche in conformità alle Linee Guida proposte da Azienda Zero con nota prot.16336/2018.

La citata delibera 1017/2018, al contenuto della quale si rimanda in toto, descrive anche i ruoli e le funzioni dei soggetti che, all'interno dell'ULSS 3, concorrono al corretto adempimento della disciplina in materia di privacy, affiancandosi al Responsabile della protezione dei dati – RPD (artt. 37-39), noto anche con l'acronimo inglese "DPO" (Data Protection Officer).

In particolare, è stato individuato un Referente Privacy aziendale.

La complessità dell'organizzazione aziendale (e la valorizzazione del concetto di Responsabilizzazione) ha reso imprescindibile oltre all'individuazione del Referente Privacy aziendale, anche la formalizzazione di una struttura di supporto che rappresenti il punto di riferimento per l'evoluzione delle disposizioni applicative che saranno necessarie nel tempo.

La composizione dell'Unità che meglio risponda alle effettive esigenze applicative richieste dalla normativa e che, al tempo stesso, garantisca un dialogo coerente ed immediato con il board di supporto al RPD, è evidentemente quella avente una formazione multidisciplinare adeguata alla mission dell'ente ovvero un gruppo di lavoro che coinvolga le seguenti aree:

- referente privacy aziendale
- area legale
- area informatica
- area della direzione medica di presidio

Questa Unità di Supporto Privacy (USP), si relaziona con la direzione e fornisce le indicazioni tecnico-giuridiche ed operative connesse all'attuazione della normativa funzionale all'assunzione delle scelte decisionali e strategiche che la disciplina richiede e richiederà.

L'USP può richiedere il coinvolgimento di altre professionalità aziendali per esigenze specifiche e congiunturali e le strutture operative e tecnico-amministrative devono garantire, nel rispetto degli impegni assunti dall'azienda in seguito all'adesione al progetto regionale, il debito supporto funzionale.

A compendio dell'assetto interno ora descritto, è stato mantenuto il collegamento operativo attivo in ambito provinciale dal 2001 in questa materia, ovvero, allo stato, dopo la riorganizzazione prevista dalla LR 19/2016, tra la ULSS 3 Serenissima e la ULSS 4 Veneto Orientale. Questa esperienza, che ha consentito di affrontare e gestire la tematica (ed altre di natura giuridico e organizzativo) con reciproca soddisfazione ed è stata riconosciuta come esempio di positiva condivisione e sinergia.

Il gruppo di lavoro provinciale il quale manterrà, ferme restando le competenze del RPD, oltre alla sua valenza di approfondimento e soluzione di casi specifici di particolare complessità, la funzione di analisi e proposta da sviluppare poi nelle rispettive sedi aziendali.

2. Riferimenti normativi

La procedura è redatta tenendo in considerazione i requisiti di cui al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito *Regolamento*) e, nello specifico, gli articoli 33 e 34, nonché le *Guidelines on Personal Data Breach Notification under Regulation 2016/679* (wp250rev.01) del WP29.

3. Definizioni

Titolare del trattamento (Art. 4, n. 7, del Regolamento): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i mezzi di 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 del trattamento (Art. 4, n. 8, del Regolamento): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Interessato: la persona fisica identificata o identificabile (**Art. 4, n. 1, del Regolamento**) a cui si riferisce il dato personale oggetto di trattamento.

Dato personale (Art. 4, n. 1, del Regolamento): 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.

Trattamento (Art. 4, n. 2, del Regolamento): 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.

Violazione dei dati personali/Data Breach (Art. 4, n. 12, del Regolamento): 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.

Notifica di una violazione dei dati personali all'Autorità di Controllo: comunicazione del Data Breach all'Autorità Garante per la protezione dei dati personali.



Comunicazione di una violazione dei dati personali all'interessato: comunicazione del *Data Breach* al soggetto i cui dati sono stati violati.

Responsabile della Protezione dei Dati (RPO): la persona fisica (o giuridica) nominata ai sensi dell'art. 37 del Regolamento, che svolge la propria attività ai sensi degli articoli 37, 38 e 39 del Regolamento medesimo o di altre disposizioni ivi contenute.

4. Destinatari

La procedura è emanata a cura dell'Azienda Ulss 3 a favore di tutti i dipendenti e collaboratori a vario titolo coinvolti nel trattamento di dati personali.

5. Ruoli e responsabilità

La tabella propone una sintesi delle attività riconducibili a ciascuna risorsa, sia interna che esterna all'Azienda, coinvolta nel processo di gestione del *Data Breach*.

Legenda di lettura della tabella (RD = Responsabilità Diretta del soggetto / PC = Per Conoscenza / C = Collaborazione / FI = Funzioni di indirizzo)

		Titolare del trattamento	Responsabile del trattamento (se coinvolto)	Responsabile della protezione dei dati
FASE ATTIVITA'	Rilevazione/Valutazione	RD (avvalendosi di Referente/ USP)	RD	FI
	Gestione	RD (avvalendosi di Referente/ USP)	C	FI
	Notifica al Garante	RD (avvalendosi di Referente/USP) (entro 72 ore)	PC	PC
	Comunicazione agli interessati	RD (avvalendosi di Referente / USP)	PC	PC
	Audit interni	RD (avvalendosi di Referente/ USP)		PC
	Archivio della documentazione	RD (avvalendosi di referente / USP)		



6. Attività operative

Le fasi di attività connesse alla gestione di eventuali violazioni di riservatezza dei dati (*Data Breach*) si sostanziano in:

1. Rilevazione / Valutazione;
2. Gestione;
3. Notifica al Garante per la protezione dei dati personali;
4. Comunicazione agli Interessati (ove necessario);
5. Pianificazione di Audit Interni;
6. Archivio della documentazione.



Rilevazione / Valutazione del *Data Breach*

Ai sensi dell'art. 4 n. 12) del Regolamento UE si intende per *Data Breach* 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.

Il Gruppo di Lavoro Articolo 29 per la protezione dei dati, nella *Opinion* 03/2014, ha identificato alcuni tipi di *Data Breach*.

In particolare, può trattarsi di:

- **"violazione della riservatezza"**: in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- **"violazione dell'integrità"**: in caso di alterazione non autorizzata o accidentale dei dati personali;
- **"perdita della disponibilità"**: in caso di perdita o distruzione dei dati personali (accidentale o non autorizzata).

A titolo esemplificativo, si riportano alcuni eventi di violazione dei dati personali per le quali è **necessario avviare la procedura**:

- perdita o furto di PC o Smartphone aziendali;
- perdita di supporti mobili quali *pen-drive* USB o *hard disk* aziendale;
- perdita di fascicoli cartacei o altra documentazione aziendale;
- invio erroneo di comunicazioni/informazioni verso l'esterno;
- attacchi informatici ai sistemi aziendali;
- accesso a dati da parte di persona non autorizzata.
- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o sia loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono stati violati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- se sono stati violati dati afferenti alla valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- se la violazione afferisce a un numero rilevante di dati;
- se l'evento riguarda il trattamento di dati personali di persone fisiche vulnerabili, in particolare minori.

Qualsiasi persona autorizzata al trattamento in Azienda, ogni qualvolta rilevi un avvenuto o potenziale *Data Breach*, **ha la responsabilità di portare l'avvenimento immediatamente all'attenzione del Titolare del trattamento.**

La comunicazione al Titolare del trattamento della violazione dei dati personali dovrà pervenire al seguente indirizzo mail: unita.supportoprivacy@aulss3.veneto.it

REGIONE DEL VENETO



ULSS3
SERENISSIMA



Parimenti, qualora la rilevazione avvenga a cura di un soggetto terzo esterno all'organizzazione (es. Responsabile del trattamento), questi informa il Titolare del trattamento senza ingiustificato ritardo, ai sensi dell'art. 33 comma 2 Regolamento (UE), con le medesime modalità di cui sopra.

Il Titolare del trattamento, avuta notizia dell'avvenuto o potenziale *Data Breach*, avvia l'istruttoria per l'identificazione dell'evento, informando del caso il personale delegato di competenza in relazione alla questione e coinvolgendo eventualmente anche il Referente aziendale ICT.

In questa fase, il Titolare del trattamento ha la possibilità di consultare il RPO per funzioni di indirizzo, anche utilizzando apposita modulistica (*allegato 1*).

Il Titolare del trattamento procede alla compilazione del *Registro Interno delle Violazioni* (*allegato 2*) indipendentemente dalle notifiche che saranno effettuate all'Autorità di controllo. Tale registro ha la funzione di documentare le valutazioni effettuate circa l'identificazione del *Data Breach*.

Gestione del *Data Breach*

Il Titolare del trattamento, laddove necessario o opportuno, procede nella gestione del *Data Breach* raccogliendo le informazioni necessarie alla descrizione dell'evento, delle misure tecniche e organizzative analogiche e/o digitali adottate e di quelle di possibile adozione per porre rimedio alla violazione e/o per attenuarne i possibili effetti negativi; ciò al fine di poter procedere nella compilazione della modulistica per la notifica al Garante.

Infine, valuta la possibilità che la violazione presenti un rischio per i diritti e le libertà degli interessati, avvalendosi del supporto del RPO nei casi di particolare complessità, per ricevere indicazioni di indirizzo.

Qualora il Titolare del trattamento dovesse ritenere non opportuno notificare la violazione di riservatezza dei dati, è necessario che le motivazioni sottostanti a tale decisione siano documentate all'interno del sopracitato *Registro Interno delle Violazioni*. A tale proposito, occorrerà descrivere i motivi per cui il Titolare del trattamento ha ritenuto che la violazione non costituisca fattore di rischio per i diritti e le libertà degli individui.

Ai fini della gestione del *Data Breach* occorre considerare se:

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

Notifica al Garante per la protezione dei dati personali

Ai sensi dell'art. 33 del Regolamento, la notifica del *Data Breach* all'Autorità di controllo è sempre obbligatoria, **salvo i casi in cui sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**. Alla comunicazione effettuata dal Titolare del trattamento dovrà essere allegata anche dettagliata relazione, comprensiva di tutti gli elementi informativi e delle valutazioni in merito effettuate.

Qualora il Titolare del trattamento ed il RPO (eventualmente consultato) abbiano opinioni discordanti circa l'insussistenza del rischio per i diritti e le libertà degli interessati, la decisione sull'opportunità di notificare la violazione dei dati personali al Garante per la protezione dei dati personali ricadrà unicamente sul Titolare del Trattamento e dovrà essere debitamente motivata.

Laddove, invece, sia rilevato un rischio per i diritti e le libertà degli interessati, il Titolare del trattamento dovrà effettuare la notifica all'Autorità Garante. In particolare, il Titolare del trattamento, utilizzando il *format* e le procedure previste dall'Autorità Garante (*allegato 3*), dovrà notificare la violazione all'Autorità di controllo senza ingiustificato ritardo e, ove possibile, **entro 72 ore** dal momento in cui ne sia venuto a conoscenza.

Contestualmente è inoltrata dal Titolare del trattamento comunicazione scritta al RPO di avvenuta notifica al Garante, per mettere il medesimo a conoscenza dell'istruttoria in atto. Qualora la notifica al Garante per la Protezione dei dati personali non sia effettuata entro 72 ore, essa dovrà essere **corredata dei motivi del ritardo**.

Se non fosse possibile fornire tutte le informazioni contestualmente, queste ultime potranno essere inviate in fasi successive senza ulteriore ingiustificato ritardo, avendo cura di dare evidenza delle motivazioni per cui tali informazioni non sono disponibili.

In questo caso sarà cura del Titolare del trattamento raccogliere le informazioni mancanti e procedere, senza ritardo, alle integrazioni eventualmente necessarie avvalendosi della collaborazione delle funzioni interessate che, a tal fine, dovranno prestare pronta, piena e fattiva disponibilità.

La mancata collaborazione delle risorse coinvolte assume rilevanza a fini disciplinari.

Ai sensi dell'art. 33 del Regolamento, la notifica all'Autorità di controllo deve contenere almeno i seguenti contenuti:

- a) descrizione della natura della violazione dei dati personali, compresi - ove possibile - le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- b) comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- c) descrizione delle probabili conseguenze della violazione dei dati personali;
- d) descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.



Comunicazione agli Interessati

Nel caso in cui la violazione dei dati personali presenti un **rischio elevato per i diritti e le libertà delle persone fisiche**, il Titolare del trattamento provvede alla comunicazione di detta violazione a tutti gli interessati coinvolti, senza ingiustificato ritardo, dandone comunicazione per conoscenza al RPD.

La comunicazione agli interessati deve descrivere, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali e deve contenere almeno le seguenti informazioni:

- a) la descrizione delle probabili conseguenze della violazione dei dati personali;
- b) 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;
- c) nome e dati di contatto del RPD.

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

- a) il Titolare del trattamento ha messo in atto misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati;
- c) detta comunicazione richiederebbe sforzi sproporzionati; in tal caso, è necessario procedere a una comunicazione pubblica, ovvero a una misura simile alternativa, tramite la quale gli Interessati sono informati con analoga efficacia.

Nel caso in cui sia il Garante per la protezione dei dati personali a ordinare con provvedimento la comunicazione del *Data Breach* agli interessati, il Titolare del trattamento pone in essere tutte le attività necessarie per ottemperare al provvedimento.

Pianificazione degli *audit*

Il RDP procederà, nel corso della propria attività di vigilanza, con cadenza almeno biennale, alla verifica sulla tenuta del Registro interno delle violazioni e delle segnalazioni di violazione dei *Data Breach*.

Archiviazione

Il Titolare del trattamento, conclusa la procedura, archivia tutte la documentazione relativa al procedimento, incluse le notifiche trasmesse al Garante per la protezione dei dati personali e agli interessati, nonché il Registro interno delle violazioni debitamente aggiornato. Il RPD potrà accedere al Registro interno delle violazioni in qualsiasi momento.



7. Modulistica allegata alla procedura

Allegato 1 - Modulo di richiesta consulenza al RPD

Allegato 2 - Registro interno delle violazioni

Allegato 3 - Modulo da inviare al Garante

8. Modifiche al presente documento

Eventuali modifiche al presente documento avranno efficacia dal momento della loro pubblicazione e si applicheranno alle nuove fattispecie di *Data Breach* che si manifesteranno, eventualmente, dopo tale efficacia, salva diversa disposizione.

REGIONE DEL VENETO



ULSS3
SERENISSIMA



Data,

Prot.n.

Al Responsabile della Protezione dei Dati

E-mail: _____

Oggetto: Richiesta consulenza al RPD per *Data Breach*

Il sottoscritto in qualità di
dell'Azienda Sanitaria
contatto telefonico e-mail
fornisce le seguenti indicazioni relative alla presunta violazione dei dati personali, oggetto
di consulenza:

QUESITO (*descrizione di alcuni elementi utili alla definizione della risposta*):

Data rilevazione della presunta violazione.....

Natura e tipologia della presunta violazione:

.....
.....
.....

Soggetti coinvolti:

.....
.....

Informazioni raccolte:

.....
.....

Azioni sviluppate:

.....
.....
.....

Azioni che il titolare intenderebbe adottare:

.....
.....
.....

Quesito:

.....
.....
.....

Firma

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.

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 qualità³ di

rappresentante legale

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) Preliminare¹

La notifica viene effettuata

- o ai sensi dell'art. 33 del RGPD
- o ai sensi dell'art. 26 d.lgs. 51/2018

o **Notifica integrativa²**

- 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).

- 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)
- 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)
- 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.

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

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.



Notifica di una violazione dei dati personali

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

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 dispone² 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*

¹Indicare 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.

Notifica di una violazione dei dati personali
art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

E) Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare, responsabile¹)

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 titolare¹
- 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 riservatezza²
- b) Perdita di integrità³
- c) Perdita di disponibilità⁴

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

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 violazione⁵

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

Notifica di una violazione dei dati personali
art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

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

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

s) Dati biometrici

t) Altro

u) Categorie ancora non determinate

13. Numero (anche approssimativo) di registrazioni⁶ 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.

Notifica di una violazione dei dati personali
art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

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 valutazione⁴

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 valutazione⁴

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 valutazione⁴

1.4. Ulteriori considerazioni sulle probabili conseguenze

Notifica di una violazione dei dati personali
art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

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

Notifica di una violazione dei dati personali
art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

H) Misure adottate a seguito della violazione

1. Misure tecniche e organizzative adottate (o di cui si propone l'adozione¹) 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'adozione¹) 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

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

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 ritiene¹ che:

- a) la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- b) la violazione non sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- 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

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

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 analogo 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 normative¹?

Sì No

Indicare a quale organismo e in virtù di quale norma

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

Sì No

Note

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

Notifica di una violazione dei dati personali
art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

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?

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

2. Indicare l’autorità di controllo capofila¹

- a) Garante per la protezione dei dati personali
- b) Altra autorità di controllo: [Selezionare]
- 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	[]	[]	[]

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

Lussemburgo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Malta	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Norvegia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Paesi Bassi	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Polonia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Portogallo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rep. Ceca	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Romania	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Slovacchia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Slovenia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Spagna	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Svezia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ungheria	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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-Württemberg) - 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)

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

- [] 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

Notifica di una violazione dei dati personali

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

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?

- a) Sì
- 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

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

- 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-Württemberg) - 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

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

- 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