



ORIGINALE

***COMUNE DI  
DIMARO FOLGARIDA***

*Provincia di Trento*

***Verbale di deliberazione n. 34  
della Giunta Comunale***

OGGETTO: Approvazione della procedura per la gestione delle violazioni dei dati personali (DATA BREACH) di cui agli articoli 33 e 34 del Regolamento UE 2016/679.

L'anno **duemilaventiquattro** addì **cinque** del mese di **marzo**, alle ore **17.20** nella sala delle riunioni della sede municipale, a seguito di regolari avvisi, recapitati a termini di legge, si è convocata oggi la Giunta Comunale.

<b>Lazzaroni</b>	<b>Andrea</b>	<b>Sindaco</b>
<b>Largaiolli</b>	<b>Alessandro</b>	<b>Vice Sindaco</b>
<b>Ghirardini</b>	<b>Alessandra</b>	<b>Assessore</b>
<b>Katzemberger</b>	<b>Marco Luigi</b>	<b>Assessore</b>
<b>Ramponi</b>	<b>Nadia</b>	<b>Assessore</b>

Assenti:

Assiste il Segretario Comunale dott.ssa Elisabetta Brighenti.

Riconosciuto legale il numero degli intervenuti, il Signor Lazzaroni Andrea, nella sua qualità di Sindaco assume la presidenza e dichiara aperta la seduta per la trattazione dell'oggetto suindicato.

Oggetto: Approvazione della procedura per la gestione delle violazioni dei dati personali (DATA BREACH) di cui agli articoli 33 e 34 del Regolamento UE 2016/679.

PREMESSO E RILEVATO CHE:

la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale; - l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea ("Carta") e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione Europea ("TFUE") stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Il Parlamento Europeo e il consiglio dell'Unione Europea hanno approvato il 27 aprile 2016 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, abrogando la Direttiva 95/46/CE.

Il 24 maggio 2016 è entrato ufficialmente in vigore il Regolamento Generale sulla Protezione dei Dati in sigla "GDPR" applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018.

Il Regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi, effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

In esecuzione del GDPR ed al fine di attuare un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, è richiesto alle aziende e alle Pubbliche Amministrazioni di approntare un piano di protezione dei dati personali che, partendo dalla mappatura e dall'analisi dei trattamenti, effettui la valutazione del rischio di violazione ed individui infine le misure volte ad eliminare o almeno ridurre il rischio stesso.

Permane comunque la possibilità che i dati personali vengano violati da parte di soggetti terzi, e che si rende quindi necessario prevedere una procedura da attuare nel caso si verificasse l'evento in questione.

PREMESSO E RILEVATO quanto sopra,

#### LA GIUNTA COMUNALE

CONSIDERATO che al fine di dare esecutività alle prescrizioni, di cui agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016, è necessario approvare il documento che contiene le procedure da attuare in caso di violazione dei dati personali (Data Breach).

EVIDENZIATO che tale documento contiene le indicazioni, le responsabilità e le azioni da attuare per la gestione della procedura in caso di possibile violazione dei dati personali, in osservanza agli obblighi relativi alla notifica all'Autorità Garante per la protezione dei dati personali e alla comunicazione all'interessato, che all'art. 33, comma 1, precisa *"In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia*

*improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.”;*

RICORDATO che tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali dell'Ente e per conto dell'ente dovranno essere informati ed osservare la procedura approvata con il presente provvedimento, puntualmente aggiornata dal Referente Privacy dell'Ente;

VISTO lo schema di procedura per la gestione della violazione dei dati personali (Data Breach) predisposto dal Consorzio dei Comuni, in qualità di Responsabile della Protezione dei dati del Comune di Dimaro Folgarida, che contiene le indicazioni, le responsabilità e le azioni da attuare per la gestione della procedura da attivare in caso di possibile violazione dei dati personali, in osservanza agli obblighi relativi alla notifica all'Autorità Garante per la protezione dei dati personali e alla comunicazione all'interessato, in ossequio alle previsioni di cui agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016;

VERIFICATO come la procedura in oggetto risulti comprensiva dei seguenti allegati:

- Registro delle violazioni dei dati personali;
- Modello di comunicazione di potenziale violazione dei dati personali al Responsabile Protezione Dati (RPD);
- Modello di comunicazione di violazione all'Autorità Garante che deve essere inviata tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo <https://servizi.gpdp.it/databreach/s/>;

ESAMINATA la proposta di cui trattasi e ritenuta la stessa meritevole di approvazione in quanto rispondente alle finalità ed ai contenuti previsti dagli artt. 33 e 34 del Regolamento (UE) 2016/679;

EVIDENZIATO che il Sindaco, con nomina di data 06.11.2023 prot. 10197, ha individuato Il Segretario Comunale, dott.ssa Elisabetta Brighenti, quale referente privacy dell'Ente, con funzioni di supporto al Titolare per l'attuazione della normativa in materia di trattamento di dati personali per gli aspetti organizzativi e tecnici e referente della gestione delle violazioni dei dati personali (Data Breach);

VISTO il Regolamento UE n. 679/2016;

VISTE le indicazioni fornite dall'Autorità Garante per la Protezione dei Dati personali e dal Responsabile Protezione Dati;

VISTA la deliberazione del Consiglio Comunale n. 02 dd 09/01/2024 di approvazione del D.U.P. 2024/2026 e la deliberazione del Consiglio comunale n. 03 dd. 09/01/2024 di approvazione del Bilancio di previsione 2024/2026 e relativi allegati;

VISTA la deliberazione della Giunta Comunale n. 63 dd 26.04.2023 relativa all'approvazione dell'atto programmatico di indirizzo per la gestione del bilancio di previsione 2023-2025 e degli atti amministrativi gestionali devoluti alla competenza dei responsabili dei servizi e dato atto che lo stesso rimane in vigore fino all'approvazione dell'atto relativo agli esercizi successivi;

VISTA la deliberazione della Giunta comunale n. 165 dd. 24/10/2023 di approvazione del Piano Integrato di Attività e Organizzazione (PIAO) 2023-2025 e rilevato che lo stesso rimane in vigore fino all'approvazione dell'atto relativo agli esercizi successivi;

VISTI:

- il Codice degli Enti locali della Regione autonoma Trentino – Alto Adige approvato con Legge regionale 3 maggio 2018 n. 2;
- la Legge provinciale 09.12.2015 n. 18 “Modificazioni della legge provinciale di contabilità 1979 e altre disposizioni di adeguamento dell’ordinamento provinciale e degli Enti locali al D.Lgs. 118/2011 e s.m. (Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli Enti locali e dei loro Organismi, a norma degli artt. 1 e 2 della Legge 05.05.2009 n. 42)”;
- il D.Lgs. 18 agosto 2000 n. 267 (Testo Unico Enti Locali) e s.m.;
- lo Statuto comunale approvato con deliberazione del Consiglio comunale n. 33 dd. 03.11.2016;
- il Regolamento di contabilità approvato con deliberazione del consiglio comunale n. 9 dd. 31.01.2018, per quanto compatibile con la normativa in materia di armonizzazione contabile;
- il Regolamento dei controlli interni approvato con deliberazione del consiglio comunale n. 2 dd. 21.02.2017;

ACQUISITO, ai sensi del combinato disposto di cui agli artt. 185 e 187 del Codice degli Enti Locali della Regione Autonoma Trentino Alto Adige approvato con L.R. 3 maggio 2018 n. 2, il parere favorevole di regolarità tecnica, attestante la regolarità e correttezza dell’azione amministrativa espresso dal Segretario Comunale;

Dato atto che l’adozione del presente provvedimento non comporta impegno di spesa e, pertanto, non risulta necessario alcun parere in ordine alla regolarità contabile del provvedimento amministrativo;

VISTO il Codice degli enti locali della Regione autonoma Trentino – Alto Adige, approvato con L.R. 3 maggio 2018, n. 2;

Visto lo Statuto comunale;

CON voti favorevoli unanimi, espressi per alzata di mano,

#### DELIBERA

1. di approvare la “Procedura per la gestione delle violazioni dei dati personali (Data Breach), di cui agli articoli 33 e 34 del Regolamento UE 2016/679”, nel testo allegato alla presente quale parte integrante e sostanziale, contenente le indicazioni, le responsabilità e le azioni da attuare per la gestione della procedura in caso di possibile violazione dei dati personali, in osservanza agli obblighi relativi alla notifica all’Autorità Garante per la protezione dei dati personali e alla comunicazione all’interessato;
2. di dare atto che il Sindaco, con nomina di data 06.11.2023 prot. 10197, ha individuato Il Segretario Comunale, dott.ssa Elisabetta Brighenti, quale referente privacy dell’Ente, con funzioni di supporto al Titolare per l’attuazione della normativa in materia di trattamento di dati personali per gli aspetti organizzativi e tecnici e referente della gestione delle violazioni dei dati personali (Data Breach);
3. di disporre che il Titolare del Trattamento Dati dell’Ente incarichi il Referente Privacy dell’ente di garantire una adeguata informazione al personale dipendente in ordine al nome del designato e alla procedura da attuare in caso si riscontrasse una potenziale violazione dei dati personali;

4. di disporre la pubblicazione del testo allegato e il modello di comunicazione di potenziale violazione dei dati personali al Responsabile Protezione Dati (RPD) nella sezione Privacy del sito istituzionale del Comune di Dimaro Folgarida;
5. di dare atto che la presente deliberazione verrà comunicata ai capigruppo consiliari contestualmente alla sua pubblicazione all'albo ai sensi dell'art. 183 comma 2 del Codice degli EE.LL. della Regione T.A.A. approvato con LR 3.5.2018 n. 2;
6. di dare evidenza, ai sensi dell'articolo 4 della L.P. 30.11.1992, n. 23, che avverso il presente provvedimento sono ammessi:
  - a) opposizione alla Giunta Comunale, durante il periodo di pubblicazione, da parte di ogni cittadino ai sensi dell'articolo 183, comma 5, del Codice degli enti locali della Regione autonoma Trentino-Alto Adige, approvato con L.R. 03.05.2018, n. 2;
  - b) ricorso giurisdizionale avanti al T.R.G.A. di Trento entro 60 giorni ex articoli 13 e 29 del D.Lgs. 02.07.2010, n. 104, da parte di chi abbia un interesse concreto ed attuale;
  - c) ricorso straordinario al Presidente della Repubblica entro 120 giorni ex articolo 8 del D.P.R. 24.11.1971, n. 1199;i ricorsi sub b) e sub c) sono alternativi.

Ai sensi dell'articolo 183, commi 1 e 3, del Codice degli enti locali della Regione autonoma Trentino-Alto Adige, approvato con L.R. 03.05.2018, n. 2, la presente deliberazione è pubblicata all'albo comunale per dieci giorni consecutivi e diverrà esecutiva il giorno successivo a quello di scadenza del periodo di pubblicazione.

Data lettura del presente verbale, lo stesso viene approvato e sottoscritto.

IL SINDACO  
Andrea Lazzaroni

IL SEGRETARIO COMUNALE  
dott.ssa Elisabetta Brighenti

RELAZIONE DI PUBBLICAZIONE

(Art. 183 del Codice degli enti locali della Regione autonoma Trentino Alto Adige approvato con Legge regionale dd. 3 maggio 2018, n. 2)

Il sottoscritto Segretario Comunale certifica che copia del presente verbale viene pubblicata all'Albo pretorio elettronico ove rimarrà esposta per 10 giorni consecutivi dal giorno **06/03/2024** al giorno **16/03/2024**.

IL SEGRETARIO COMUNALE  
dott.ssa Elisabetta Brighenti

Il sottoscritto Segretario Comunale dichiara, ai sensi dell'art. 183 comma 3 del Codice degli enti locali della Regione autonoma Trentino Alto Adige approvato con Legge regionale dd. 3 maggio 2018, n. 2, che la presente deliberazione dichiarata **esecutiva a pubblicazione avvenuta** ad ogni effetto di legge.

IL SEGRETARIO COMUNALE  
dott.ssa Elisabetta Brighenti

Oggetto: Approvazione della procedura per la gestione delle violazioni dei dati personali (DATA BREACH) di cui agli articoli 33 e 34 del Regolamento UE 2016/679.

**SERVIZIO SEGRETERIA**

Si dichiara che, con riguardo al presente provvedimento, non sussistono nei confronti del responsabile del procedimento, cause di conflitto di interesse, anche potenziali, che richiedono l'obbligo di astensione ai sensi della normativa vigente.



IL SEGRETARIO COMUNALE

dott.ssa Brighenti Elisabetta

**SERVIZIO SEGRETERIA**

In relazione al combinato disposto ai sensi degli Artt. 185 e 187 del Codice degli Enti Locali della Regione Trentino Alto - Adige, approvato con L.R. 3 maggio 2018 n. 2, vista la proposta di deliberazione e la documentazione di supporto ed istruttoria, si esprime parere favorevole in ordine alla regolarità tecnica ai fini amministrativi del presente atto.



IL SEGRETARIO COMUNALE

dott.ssa Brighenti Elisabetta

Dimaro Folgarida lì, 04 marzo 2024



# **COMUNE DI DIMARO FOLGARIDA**

PROVINCIA DI TRENTO

## **PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)**

(approvata con deliberazione della Giunta Comunale n. \_\_\_\_ d.d. \_\_\_\_\_)

### **INDICE**

<b>1. SCOPO</b>	<b>2</b>
<b>2. AGGIORNAMENTO</b>	<b>2</b>
<b>3. DEFINIZIONI</b>	<b>2</b>
<b>4. ORGANIZZAZIONE DELLE ATTIVITÀ DI GESTIONE DELL'EVENTO VIOLAZIONE DEI DATI PERSONALI</b>	<b>3</b>
<b>5. GESTIONE DELLE ATTIVITÀ CONSEGUENTI AD UNA POSSIBILE VIOLAZIONE DI DATI PERSONALI</b>	<b>3</b>
<b>6. NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ GARANTE</b>	<b>3</b>
<b>7. COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI AGLI INTERESSATI</b>	<b>4</b>
<b>8. COMPILAZIONE DEL REGISTRO DELLE VIOLAZIONI DEI DATI PERSONALI</b>	<b>4</b>



## 1 Scopo

Il presente documento contiene le indicazioni, le responsabilità e le azioni da attuare per la gestione della procedura da attivare in caso di possibile violazione dei dati personali, in osservanza agli obblighi relativi alla notifica all'Autorità Garante per la protezione dei dati personali e alla comunicazione all'interessato, in ossequio alle previsioni di cui agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016.

Tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali dell'Ente devono essere informati e osservare la presente Procedura.

## 2 Aggiornamento

Il Referente privacy dell'Ente, nel caso di variazioni organizzative e/o normative, aggiorna la presente procedura e la propone in approvazione all'Organo competente affinché la renda esecutiva.

## 3 Definizioni

Le seguenti definizioni dei termini utilizzati in questo documento sono tratte dall'articolo 4 del Regolamento europeo n. 679 del 2016:

«**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;

«**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;

«**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;

«**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 in formato elettronico e/o cartaceo;

«**Responsabile della Protezione dei Dati**»: incaricato di assicurare la corretta gestione dei dati personali nell'Ente;

«**Autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR dell'UE.

## **4 Organizzazione delle attività di gestione dell'evento violazione dei dati personali**

Il Titolare deve:

- designare un Referente della gestione delle violazioni dei dati personali (di seguito Referente Data Breach), figura che potrebbe coincidere con il Referente privacy dell'Ente.
- comunicare i nomi dei designati a tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali dell'Ente;
- avvalendosi del Referente Data Breach, predisporre il Registro delle violazioni dei dati personali.

## **5 Gestione delle attività conseguenti ad una possibile violazione di dati personali**

Il soggetto che, a diverso titolo o in quanto autorizzato al trattamento di dati personali di cui è titolare l'Ente, viene a conoscenza di una possibile violazione dei dati personali, deve immediatamente segnalare l'evento al Referente Privacy dell'Ente e al Referente Data Breach e fornire loro la massima collaborazione.

La mancata segnalazione del suddetto evento comporta a diverso titolo responsabilità a carico del soggetto che ne è a conoscenza.

Il Referente Data Breach, se del caso avvalendosi del Gruppo di gestione delle violazioni dei dati personali, deve:

- adottare le Misure di sicurezza informatiche e/o organizzative per porre rimedio o attenuare i possibili effetti negativi della violazione dei dati personali e, contestualmente, informare immediatamente il Responsabile della Protezione dei Dati per una valutazione condivisa;
- condurre e documentare un'indagine corretta e imparziale sull'evento (aspetti organizzativi, informatici, legali, ecc.) attraverso la compilazione del "Modello di potenziale violazione di dati personali al Responsabile Protezione Dati";
- riferire i risultati dell'indagine inviando il modello all'indirizzo [serviziordp@comunitrentini.it](mailto:serviziordp@comunitrentini.it) al Responsabile della Protezione dei Dati, al Referente privacy dell'Ente e il Titolare.

Il Responsabile della Protezione dei Dati, ricevuti i risultati dell'indagine, analizza l'accaduto e formula un parere in merito all'evento, esprimendo la propria valutazione, non vincolante, che lo stesso configuri in una violazione dei dati personali e che possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche. Tale parere è quindi trasmesso al Referente Data Breach, al referente Privacy dell'Ente (qualora individuato in un soggetto distinto) nonché al Titolare.

## **6 Notifica della violazione dei dati personali all'Autorità Garante**

Il Titolare, tenuto conto del parere formulato dal Responsabile della Protezione dei Dati, e dalle valutazioni fatte congiuntamente dal Referente della gestione delle violazioni dei dati personali e dal Referente Privacy dell'Ente (qualora soggetto distinto dal primo), se ritiene accertata la violazione dei dati personali e che la stessa possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche, notifica tale violazione avvalendosi del "Modello comunicazione violazione all'Autorità Garante".

La notifica deve essere effettuata senza ingiustificato ritardo dall'accertamento dell'evento e, ove possibile, entro 72 ore dall'accertamento dello stesso con le modalità e i contenuti previsti dall'art. 33 del Regolamento europeo n. 679 del 2016.

## **7 Comunicazione della violazione dei dati personali agli interessati**

Il Titolare, accertata la violazione dei dati personali e ritenendo che la stessa possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte, oltre alla notifica di cui al punto 6, decide le modalità di comunicazione di tale violazione agli interessati, come previsto dall'art. 34 del Regolamento europeo n. 679 del 2016.

## **8 Compilazione del Registro delle violazioni dei dati personali**

Il Titolare, avvalendosi del Referente Data Breach, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nel Registro delle violazioni dei dati personali.

Tale documento è tenuto e implementato dal Referente Data Breach e consente all'autorità di controllo di verificare il rispetto dall'art. 33 del Regolamento europeo n. 679 del 2016.

Per la redazione del registro è possibile ricorrere al sistema di fascicolazione se disponibile nel programma di gestione documentale dell'Ente o ad un file Excel.

Registro delle violazioni dei dati - COMUNE DI DIMARO FOLGARIDA								
NR.	Data accadimento	Data comunicazione al referente interno	Breve descrizione evento	Servizio/Ufficio competente al trattamento	Coinvolgimento RPD: SI/NO	Azioni / Misure adottate	Notifica al Garante SI/NO e data	Comunicazione agli interessati SI/NO e data
1								
2								
3								
4								
5								
6								

## POTENZIALE VIOLAZIONE DI DATI PERSONALI

### MODELLO DI COMUNICAZIONE AL RESPONSABILE DELLA PROTEZIONE DEI DATI

Ente \_\_\_\_\_  
Referente \_\_\_\_\_  
Privacy \_\_\_\_\_  
Telefono \_\_\_\_\_ Email \_\_\_\_\_

#### Breve descrizione della violazione dei dati personali

#### Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

#### Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca di dati?

- ☐ Il \_\_\_\_\_
- ☐ Tra il \_\_\_\_\_ e il \_\_\_\_\_
- ☐ In un tempo non ancora determinato
- ☐ È possibile che sia ancora in corso

**Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)**

**Modalità di esposizione al rischio: tipo di violazione**

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e non li ha l'autore della violazione)
- ☐ Altro \_\_\_\_\_

**Dispositivo o strumento oggetto della violazione**

- ☐ Computer
- ☐ Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di backup
- ☐ Documento cartaceo
- ☐ Software \_\_\_\_\_
- ☐ Servizio informatico \_\_\_\_\_
- ☐ Altro \_\_\_\_\_

**Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?**

- ☐ Numero \_\_\_\_\_ di persone
- ☐ Circa \_\_\_\_\_ persone
- ☐ Un numero (ancora) sconosciuto di persone

**Che tipo di dati sono oggetto di violazione?**

- ☐ Dati anagrafici/codice fiscale
- ☐ Dati di accesso e di identificazione (*username, password, customer ID, altro*)
- ☐ Dati relativi a minori

- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico, o sindacale
- ☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- ☐ Dati giudiziari
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ Altro \_\_\_\_\_

**Fornitori o soggetti esterni coinvolti**

**Misure tecniche, informatiche e organizzative applicate ai dati oggetto di violazione**

Luogo e data \_\_\_\_\_

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<sup>1\*</sup> ..... Nome<sup>1\*</sup> .....

E-mail<sup>2\*</sup> .....

nella sua qualità<sup>3</sup> di

☐ rappresentante legale

☐ delegato del rappresentante legale

Cognome<sup>4\*</sup> ..... Nome<sup>4\*</sup> .....

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.

<sup>1</sup> 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).

<sup>2</sup> 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".

<sup>3</sup> 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".

<sup>4</sup> 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<sup>1</sup>

**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**<sup>2</sup>

- o c) fascicolo n. <sup>3\*</sup> ..... PIN <sup>3\*</sup> .....

<sup>1</sup> 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.

<sup>2</sup> Il titolare del trattamento, avvalendosi delle previsioni di cui all'art. 33 par. 4 del Regolamento, integra una precedente notifica.

<sup>3</sup> 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](http://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](http://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<sup>1\*</sup> ..... Soggetto privo di C.F./P.IVA italiana ☐  
Stato\* .....  
Provincia\* ..... Comune\* ..... CAP\* .....  
Indirizzo\* .....  
Telefono\* .....  
E-mail<sup>2\*</sup> .....  
PEC<sup>2\*</sup> .....

<sup>1</sup> 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".

<sup>2</sup> 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<sup>1\*</sup> .....  
Codice Fiscale/P.IVA\* ..... Soggetto privo di C.F./P.IVA italiana ☐  
Stato\* .....  
Provincia\* ..... Comune\* ..... CAP\* .....  
Indirizzo\* .....  
Telefono\* .....  
E-mail<sup>2\*</sup> .....  
PEC<sup>2\*</sup> .....

<sup>1</sup> 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).

<sup>2</sup> 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).

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

- i cui dati di contatto sono stati già comunicati con la comunicazione protocollo<sup>1\*</sup> n.....
- i cui dati di contatto sono stati già comunicati al Garante, ma al momento non si dispone<sup>2</sup> 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\* .....

---

<sup>1</sup>Indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD.

<sup>2</sup> 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, responsabile<sup>1</sup>)

Denominazione<sup>2\*</sup> .....  
Codice Fiscale<sup>3\*</sup> ..... Soggetto privo di C.F./P.IVA ☐  
Ruolo O Contitolare O Responsabile

Denominazione<sup>2\*</sup> .....  
Codice Fiscale<sup>3\*</sup> ..... Soggetto privo di C.F./P.IVA ☐  
Ruolo O Contitolare O Responsabile

Denominazione<sup>2\*</sup> .....  
Codice Fiscale<sup>3\*</sup> ..... Soggetto privo di C.F./P.IVA ☐  
Ruolo O Contitolare O Responsabile

<sup>1</sup> 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.

<sup>2</sup> Nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale.

<sup>3</sup> 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<sup>1</sup>
- ☐ 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<sup>2</sup>
- ☐ b) Perdita di integrità<sup>3</sup>
- ☐ c) Perdita di disponibilità<sup>4</sup>

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 violazione<sup>5</sup>

### 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 registrazioni<sup>6</sup> 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 valutazione<sup>4</sup>

**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<sup>4</sup>

**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<sup>4</sup>

**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'adozione<sup>1</sup>) 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<sup>1</sup>) per prevenire simili violazioni future**

**3. Allegati**

☐ Intendo allegare un documento contenente ulteriori informazioni

---

<sup>1</sup> 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<sup>1</sup> 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

## 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 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<sup>1</sup>?**

☐ 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

---

<sup>1</sup>. 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 capofila<sup>1</sup>**

- ☐ 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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Austria	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Belgio	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bulgaria	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cipro	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Croazia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Danimarca	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Estonia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Finlandia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Francia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Germania	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Grecia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Irlanda	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Islanda	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lettonia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Liechtenstein	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lituania	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 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 (CNPDP)
- ☐ 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 (CNPDP)
- ☐ 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