



COMUNE DI TEGLIO VENETO

Città Metropolitana di Venezia

DISCIPLINARE PER LA

PROCEDURA DI GESTIONE DEI DATA BREACH

Sommario

1. NORMATIVA DI RIFERIMENTO	3
2. PREMESSA E SCOPO	3
3. CAPO DI APPLICAZIONE	4
4. DEFINIZIONI GENERALI	4
5. DESTINATARI DELLA PROCEDURA	4
6. DOCUMENTAZIONE DELLE ATTIVITA' SVOLTE CON RIFERIMENTO ALLA GESTIONE DEI DATA BREACH	5
7. TIPOLOGIE DI VIOLAZIONE	5
8. FASI DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI	5
a. FASE 1: Scoperta e rilevazione del data breach	5
b. FASE 2: Qualificazione e valutazioni iniziali	7
c. FASE 3: Valutazione della gravità della violazione e stima del rischio per gli interessati	7
d. FASE 4: Notifica all'autorità di controllo	8
e. FASE 5: Comunicazione agli interessati	8
f. FASE 6: Risoluzione dell'incidente	9
9. ALLEGATI	11
a. Fac simile di notifica all'Autorità di Controllo	11
b. Esempi commentati di violazione	12
c. Modello di comunicazione agli interessati della violazione dei dati	14

1. NORMATIVA DI RIFERIMENTO

La normativa di riferimento per la stesura del presente documento è la seguente:

Regolamento Europeo 679/2016 (o anche GDPR)	Regolamento generale sulla protezione dei dati
D.lgs. n.196/2003 e s.m.i.	Codice in materia di protezione di dati personali
Working Party 250 adottate il 3 ottobre 2017	<i>Linee Guida Sulla Notifica Delle Violazioni Dei Dati Personali Ai Sensi Del Regolamento (Ue) 2016/679</i>
Linee guida adottate dall'EDPB n. 1/2021	<i>Guidelines on examples regarding Data Breach Notification</i>
Raccomandazioni adottate dall'EDPB il 20 dicembre 2013	<i>Recommendations for a methodology of the assessment of severity of personal data breaches</i>

2. PREMESSA E SCOPO

La presente procedura ha lo scopo di determinare la procedura per la gestione e le segnalazioni dei **Data Breach** in conformità al GDPR. In particolare, è volta a stabilire un flusso di informazioni e attività da attuare in tali casi.

Si precisa che il GDPR definisce il Data Breach, ossia la violazione dei dati personali, come **una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati**.

A titolo esemplificativo ma non esaustivo, si ricorda che possono configurare violazioni di dati personali le seguenti casistiche:

- cyber-attacco mediante cui vengono rubati dati personali;
- sottrazione/perdita di materiale/dispositivi contenenti dati personali (es. pc, chiavette, documenti cartacei,...);
- furto di documentazione negli uffici o un furto di posta nella cassetta postale o il recupero di documenti non distrutti gettati nei rifiuti contenente dati personali;
- invio di un messaggio di posta elettronica contenente una lista di interessati con indicazione dei loro recapiti a destinatario errato;
- condivisione/diffusione di verbali riservati con soggetti non autorizzati;
- attacco ransomware che causa la crittografia dei dati e, dunque, la loro indisponibilità foss'anche temporanea;
- la serratura di un armadio contenente archivi cartacei relativi alle carriere del personale tecnico amministrativo è stata forzata;
- circostanze impreviste quali incendi o allagamenti.

È opportuno precisare, inoltre, che ai sensi del Considerando 85 del GDPR, una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Alla luce di tali disposizioni normative, il Titolare del Trattamento è tenuto a segnalare, ove necessario sulla base della normativa stessa e in accordo con le linee direttive della presente procedura, le violazioni che avesse subito all'Autorità di controllo, Autorità che per lo Stato Italiano è da identificarsi nel Garante per la Protezione dei Dati Personali. Inoltre, nell'ipotesi in cui la violazione comporti un rischio elevato per i diritti e le libertà delle persone fisiche alla segnalazione dovrà seguire specifica comunicazione agli interessati.

Si segnala, infine, che in caso di mancata segnalazione il Titolare del Trattamento è passibile di sanzione ai sensi dell'art. 83 del GDPR.

3. CAPO DI APPLICAZIONE

La presente procedura si applica a tutte le ipotesi di violazioni di dati personali trattati dall'Ente, siano esse sospette o confermate. Tali ipotesi devono essere prontamente individuate e vagliate dall'Ente quand'anche quest'ultimo trattasse suddetti dati in qualità di mero Responsabile del Trattamento ai sensi dell'art. 28 del GDPR:

4. DEFINIZIONI GENERALI

Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Dato personale: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. In tale categoria rientrano per esempio: documenti di identità, indirizzi mail, coordinate bancarie, numeri di telefono,...

Dati particolari: i 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, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale. In tale categoria rientrano per esempio: infortuni, stato di salute, iscrizione al sindacato, gravidanza,...

Dati giudiziari: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza. In tale categoria rientrano per esempio: informazioni del casellario, DASPO,...

Titolare: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile esterno del trattamento: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali.

Autorizzato: la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Designato. In tale categoria rientra il personale e i collaboratori dell'Ente.

Interessato: la persona fisica, cui si riferiscono i dati personali. In tale categoria rientrano per esempio: clienti, potenziali clienti, candidati, dipendenti,...

5. DESTINATARI DELLA PROCEDURA

L'Ente, coadiuvato dal Responsabile Privacy e dal Responsabile della Protezione dei Dati (DPO), ha il compito di assicurare l'attuazione della presente procedura e la corretta gestione delle violazioni di dati personali.

Ne consegue che la presente procedura dovrà essere condivisa con tutto il personale e da questo rispettata. Si precisa che laddove ci si riferisce al personale nella presente procedura ci si intende riferire, a titolo non esaustivo, ai seguenti soggetti: dipendenti, tirocinanti, consulenti, collaboratori, interinali,...

Inoltre, la stessa necessita di essere messa a disposizione dei fornitori che svolgano anche il ruolo di Responsabili o sub-responsabili del Trattamento.

6. DOCUMENTAZIONE DELLE ATTIVITA' SVOLTE CON RIFERIMENTO ALLA GESTIONE DEI DATA BREACH

Il Titolare del Trattamento dovrà mantenere aggiornato nel corso di tutta la gestione del Data Breach il Registro delle Violazioni presente in One 679. **Il registro delle Violazioni deve essere continuamente aggiornato e messo a disposizione del Garante** qualora l'Autorità chieda di accedervi.

L'incarico di mantenere aggiornato tale documento viene affidato al Referente Privacy. Tale documento insieme alla documentazione raccolta, ricevuta o prodotta durante la gestione di ciascuna violazione dovrà essere conservata in maniera strutturata e archiviata agli atti dell'Ente.

7. TIPOLOGIE DI VIOLAZIONE

A seconda dei casi una violazione può comportare:

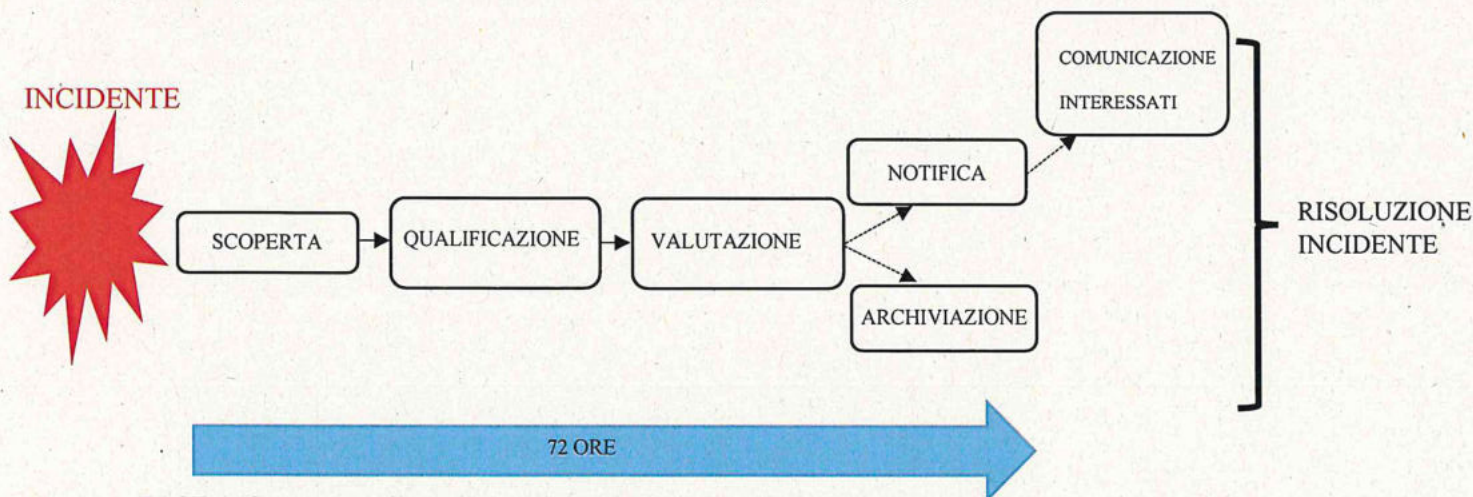
1. una perdita di riservatezza dei dati personali: quanto si ha una divulgazione dei dati personali o accesso agli stessi non autorizzato o accidentale;
2. una perdita di integrità: quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
3. una perdita di disponibilità: quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

È opportuno, in ogni caso, sottolineare che vi possono essere ipotesi in cui le precedenti casistiche si combinano nel contesto di una unica violazione. A titolo esemplificativo si consideri un attacco hacker che comporti sia la cancellazione dei dati a disposizione dell'Ente sia una loro contestuale diffusione nel dark web così determinando una perdita di riservatezza e integrità.

A di là delle conseguenze che una violazione di dati personali può generare, si significa che risulta di primaria importanza che la stessa venga riconosciuta e presa in considerazione dal Titolare del Trattamento affinché possano essere poste in essere contromisure o attività preventive.

8. FASI DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

Di seguito si riporta lo schema delle fasi in cui si articola il processo di gestione dei Data Breach.



Qualunque autorizzato che accerti o riceva comunicazione circa un incidente di sicurezza che possa comportare una violazione di dati personali è tenuto a segnalarlo **immediatamente** al proprio Superiore gerarchico il quale sarà tenuto ad informarne il Referente Privacy e/o il DPO.

Nell'ipotesi in cui una violazione di dati personali dovesse verificarsi e/o essere scoperta al di fuori del normale orario di servizio, la stessa deve essere segnalata appena possibile e, in ogni caso, non appena si rientri in servizio.

In linea generale, il Titolare del Trattamento può essere informato di un incidente di sicurezza:

- dal personale/collaboratori dell'Ente;
- dal DPO;
- dal Responsabile del Trattamento o da un soggetto esterno;
- da un interessato;
- da articoli di stampa.

In linea generale, a seguito della segnalazione al proprio superiore gerarchico, l'autorizzato non è chiamato ad intraprendere ulteriori azioni in merito alla violazione a meno che il superiore gerarchico/Referente Privacy/DPO non ravvisi la necessità di un ulteriore coinvolgimento.

Ricevuta la segnalazione, il Superiore gerarchico, con l'ausilio eventualmente dell'Amministratore di Sistema, dovrà raccogliere tutte le informazioni necessarie per segnalare i fatti al Referente Privacy e/o al DPO. In particolare, sarà opportuno che lo stesso raccolga le seguenti informazioni, che a loro volta saranno inserite dal Superiore gerarchico stesso o dal Referente privacy nel registro delle violazioni presente in One679:

- Data evento anomalo;
- Data presunta di avvenuta violazione;
- Data e ora in cui si è avuta conoscenza della violazione;
- Fonte segnalazione;
- Tipologia violazione;
- Tipologia di informazioni coinvolte;
- Descrizione dell'evento anomalo avendo cura di evidenziare se lo stesso sia ancora in corso;
- Categorie e numero, se noto, di Interessati coinvolti;
- Numerosità di Dati Personali di cui si presume una violazione;
- Indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di Device Mobili;
- Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione;
- Eventuali azioni già intraprese per porre rimedio alla violazione;
- Eventuali soggetti terzi coinvolti (es. fornitori).

Le segnalazioni del Superiore gerarchico devono essere tempestivamente comunicate al Referente Privacy e/o al DPO ed in ogni caso entro 12 ore dalla conoscenza della violazione da parte del Superiore gerarchico. Tale comunicazione dovrebbe avvenire ove possibile a mezzo PEC o comunque tramite i canali istituzionali riferibili ai destinatari. Qualora il Superiore gerarchico non avesse provveduto a segnalare l'evento al DPO, il Referente privacy vi dovrà provvedere immediatamente.

Si ricorda che in ipotesi di violazione di dati personali la celerità nella gestione dell'evento è fondamentale al fine di rispettare gli obblighi gravanti sul Titolare del Trattamento. Ciò in quanto lo stesso è chiamato a **notificare la violazione dei dati personali all'Autorità di Controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che il Titolare del Trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite nelle fasi successive senza ulteriore ingiustificato ritardo.

Al fine di stabilire il momento di conoscenza della violazione da parte del Titolare del Trattamento si fa riferimento al momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali.

Il Referente Privacy dovrà fin da subito attenzionare della vicenda i vertici direzionali dell'Ente e provvedere ad aggiornare gli stessi anche con riferimento alle fasi successive del processo di gestione del Data Breach.

b. FASE 2: Qualificazione e valutazioni iniziali

Al ricevimento della segnalazione il Referente Privacy con il supporto del DPO e, se del caso, dell'Amministratore di sistema dovrà valutare se la violazione sia ancora in corso e, in tale ipotesi, stabilire le misure appropriate da adottare, mantenendo sul punto aggiornato il Registro delle Violazioni.

Qualora la violazione riguardi dati trattati dall'Ente in qualità di Responsabile esterno del Trattamento, le informazioni di cui all'elenco riportato nella Fase 1 dovranno essere immediatamente condivise con il Titolare del Trattamento. In tali ipotesi l'Ente dovrà supportare il Titolare nelle diverse fasi di gestione del Data Breach.

La Fase 2 del processo di gestione dovrà essere portata a termine **entro le 24 ore dalla conoscenza della violazione da parte del Superiore gerarchico.**

c. FASE 3: Valutazione della gravità della violazione e stima del rischio per gli interessati

La Fase 3 sarebbe opportuno che venisse condotta **entro le 48 ore dalla conoscenza della violazione da parte del Superiore gerarchico** al fine di permettere di inviare tempestivamente l'eventuale comunicazione all'Autorità Garante.

Il Referente Privacy, coadiuvato dalle altre funzioni competenti e dal DPO, provvederà, redigendo apposito documento riepilogativo che rimarrà agli atti, ad integrare le informazioni finora raccolte al fine di stabilire:

- **Tipologia del breach** (riservatezza, integrità, disponibilità) e presenza di un eventuale **intento malevolo**.
- **Natura e volume dei dati** coinvolti dal breach.
- **Facilità di identificazione** degli interessati.
- **Criticità delle conseguenze per gli interessati.**
- **Numero degli interessati** coinvolti del breach.
- **Caratteristiche del Titolare** dei dati oggetto del breach.
- **L'eventuale intellegibilità dei dati coinvolti.**

La valutazione della gravità della violazione verrà condotta sulla base della metodologia definita dall'ENISA nel documento *Recommendations for a methodology of the assessment of severity of personal data breaches*.

La violazione deve essere valutata secondo i livelli di rischio:

- NULLO
- BASSO
- MEDIO
- ALTO
- MOLTO ALTO

L'analisi permetterà di stabilire in primo luogo la necessità di attivare le procedure di comunicazione e di notifica all'Autorità Garante. **Tale notifica si renderà necessaria in ipotesi di violazioni di gravità MEDIO-ALTA.** Rimane inteso che la metodologia sopracitata non è in grado di coprire tutte le possibili casistiche del caso concreto e, dunque, il Titolare del Trattamento può considerare di modificare i punteggi attribuiti alle categorie della metodologia in base agli elementi concreti che caratterizzano l'evento. In tali ipotesi, qualora gli elementi del caso concreto dovessero condurre a non ritenere necessaria la comunicazione nonostante il punteggio ottenuto, sarà opportuno che le motivazioni alla base della mancata segnalazione sia adeguatamente documentate e giustificate.

Fin da tale Fase, l'Ente dovrebbe provvedere ad individuare le misure tecniche ed organizzative per porre rimedio alla violazione ad attenuarne gli effetti negativi nonché quelle per prevenire che simili violazioni future avvengano.

d. FASE 4: Notifica all'autorità di controllo

Qualora, in base alle valutazioni di cui alla Fase 3, si stabilisse la necessità di effettuare una segnalazione all'Autorità Garante sarà necessario che la procedura di segnalazione sia effettuata collegandosi al portale dell'Autorità stesse fornendo le informazioni presenti anche nell'**Allegato A**. Per ultimare la procedura stessa sarà necessario attenersi alle istruzioni del portale riportate nella seguente pagina web <https://www.garanteprivacy.it/regolamentoue/databreach>.

Sarà compito del Referente Privacy, unitamente ai referenti interni incaricati della gestione della privacy, e con la costante supervisione del DPO, provvedere alla redazione della notifica e curarne il relativo invio in concerto con la Direzione.

La notifica dovrà pervenire all'Autorità possibilmente entro le 72 ore dall'avvenuta conoscenza della violazione. Diversamente si dovrà provvedere a motivare il ritardo nella segnalazione.

Qualora il Titolare non sia già in possesso di tutti gli elementi utili per effettuare una descrizione completa ed esaustiva dell'infrazione, può adottare alcune tecniche o modalità che permettono di bilanciare le esigenze di celerità del messaggio con quelle di una sua sostanziale accuratezza e completezza.

Approssimazione: il Titolare che non sia ancora in grado di conoscere con certezza il numero di persone e di dati personali interessati dalla violazione può comunicarne in prima battuta un ammontare approssimativo, provvedendo a specificare il numero esatto a seguito di accertamenti.

Notificazione in fasi: in questo caso il Titolare, per la complessità o estensione della violazione, potrebbe non essere in grado di fornire con immediatezza all'Autorità tutte le informazioni necessarie. Potrà allora ottemperare agli obblighi di notifica comunicando, dopo una prima e rapida notifica preliminare, tutte le informazioni per fasi successive, aggiornando di volta in volta l'Autorità sui nuovi riscontri.

Notifica differita: dopo le 72 ore previste dall'art. 33 del GDPR. È il caso in cui, per esempio, un'impresa subisca violazioni ripetute, ravvicinate e di simile natura che interessino un numero elevato di soggetti. Al fine di evitare un aggravio di oneri in capo al Titolare e l'invio scaglionato di un numero elevato di notificazioni tra loro identiche, il Titolare è autorizzato ad eseguire un'unica notifica aggregata di tutte le violazioni occorse nel breve periodo di tempo (anche se superi le 72 ore), purché la notifica motivi le ragioni del ritardo.

Una volta effettuata la notifica il Referente Privacy e il DPO avranno cura di mantenere i rapporti e i contatti con l'Autorità Garante supportandola in ogni operazione e rispettando eventuali indicazioni dalla stessa provenienti.

e. FASE 5: Comunicazione agli interessati

Il GDPR stabilisce 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 comunichi la violazione agli interessati senza ingiustificato ritardo. Tra i potenziali impatti da considerare sotto tale profilo si richiamo, a titolo esemplificativo, i seguenti:

- Danni economici o sociali
- Danni fisici, materiali o morali
- Perdita del controllo dei dati
- Limitazione dei diritti
- Discriminazione
- Furto o usurpazione d'identità
- Perdite finanziarie
- Decifratura non autorizzata della Pseudoanimizzazione
- Pregiudizio alla reputazione
- Perdita di riservatezza dei dati protetti da segreto professionale (sanitari, giudiziari)
- Conoscenza da parte di terzi non autorizzati

Al fine di valutare se la comunicazione agli interessati sia dovuta si dovranno considerare sia gli esiti delle valutazioni di cui alla Fase 3 sia le ipotesi esemplificate contenute nell'**Allegato B** della presente procedura (tratte dal WP 250) e quelle presenti nelle *Guidelines 01/2021 on examples regarding Data Breach Notification*.

La comunicazione all'interessato non è tuttavia richiesta se si ravvisano uno dei seguenti casi:

- quando il Titolare del Trattamento ha messo in atto, e applicato ai dati che sono stati oggetto di violazione, tutte le necessarie misure tecniche e organizzative di protezione, comprese quelle destinate a rendere i dati personali incomprensibili ai soggetti non autorizzati (come, ad esempio, la cifratura delle informazioni).
- quando il Titolare del Trattamento abbia successivamente adottato misure per scongiurare il verificarsi di un rischio elevato per i diritti e le libertà degli interessati.
- quando la comunicazione stessa richiederebbe sforzi sproporzionati e, in tal caso, si può procedere a una comunicazione pubblica o ad altra soluzione analoga, così da informare gli interessati in maniera ugualmente efficace.

Rimane, in ogni caso, possibile per il Titolare ottenere, all'atto di notifica della violazione, una consulenza da parte della stessa Autorità di Controllo circa la necessità di informare le persone interessate.

Qualora fosse necessario operare la comunicazione agli interessati, devono sempre essere **privilegiate modalità di comunicazione diretta con i soggetti interessati (quali email, SMS o messaggi diretti)**. Il messaggio dovrebbe essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di *update* generali o *newsletter*, che potrebbero essere facilmente fraintesi dai lettori. Inoltre, dovrebbe tenere conto di possibili formati alternativi di visualizzazione del messaggio e delle diversità linguistiche dei soggetti riceventi (es. l'utilizzo della lingua madre dei soggetti riceventi rende il messaggio immediatamente comprensibile).

Inoltre, nelle ipotesi in cui si ritenga eccessivamente onerosa una segnalazione diretta, le modalità di comunicazione pubblica devono mantenere lo stesso grado di efficacia conoscitiva del contatto diretto con l'interessato. Così, mentre può ritenersi adeguata la comunicazione fornita attraverso evidenti *banner* o notifiche disposte sui siti web, non lo sarà se questa sia limitata all'inserimento della notizia in un blog o in una rassegna stampa.

La comunicazione agli interessati dovrà avere i seguenti contenuti:

- descrizione con un linguaggio semplice e chiaro della natura della violazione dei dati personali.
- nome e dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.
- descrizione delle probabili conseguenze della violazione dei dati personali.
- descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

La predisposizione del messaggio agli interessati e la scelta delle modalità di comunicazione sono rimesse al Referente Privacy coadiuvato dal DPO e dovranno essere avvallate dalla Direzione.

All'**Allegato C** è possibile reperire una bozza di comunicazione agli interessati.

f. FASE 6: Risoluzione dell'incidente

Il Titolare del Trattamento, all'esito dell'incidente di sicurezza – a prescindere da una segnalazione all'Autorità Garante – e in virtù di quanto eventualmente precisato all'atto di notifica all'Autorità di Controllo, dovrà verificare l'efficacia delle misure preventive già adottate nonché implementare le stesse con le misure tecniche e organizzative necessarie sia per porre rimedio alla violazione e/o attenuarne gli effetti sia per prevenire eventi simili.

Occorrerà quindi revisionare/correggere le lacune di sicurezza identificate, considerando, a titolo esemplificativo:

- le attuali misure di sicurezza;
- i metodi di trasmissione e la loro sicurezza;

- il livello di condivisione dei dati valutando l'effettiva necessità di tale condivisione;
- la necessità di condurre o aggiornare eventuali valutazioni d'impatto sulla protezione dei dati;
- il luogo e le modalità di archiviazione;
- la necessità di aggiornare le procedure interne e/o la modulistica;
- la formazione del personale in materia di protezione dei dati e il suo aggiornamento;
- la conoscenza delle procedure interne e dei regolamenti in capo al personale.

9. ALLEGATI

- a. Fac simile di notifica all'Autorità di Controllo
-



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.gdpd.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

- ☐ a) Completa
- ☐ b) Preliminare¹

La notifica viene effettuata

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

o Notifica integrativa²

- ☐ 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:

- ☐ a) Fornire ulteriori informazioni senza completare il processo di notifica
- ☐ b) Fornire ulteriori informazioni e completare il processo di notifica
- ☐ c) Completare il processo di notifica senza fornire ulteriori informazioni
- ☐ 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 (INIEPEC). 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.iniepec.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-mail²*
PEC²*

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

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 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 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	☐	☐	☐
Malta	☐	☐	☐
Norvegia	☐	☐	☐
Paesi Bassi	☐	☐	☐
Polonia	☐	☐	☐
Portogallo	☐	☐	☐
Rep. Ceca	☐	☐	☐
Romania	☐	☐	☐
Slovacchia	☐	☐	☐
Slovenia	☐	☐	☐
Spagna	☐	☐	☐
Svezia	☐	☐	☐
Ungheria	☐	☐	☐

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

- ☐ Austria - Data Protection Authority
- ☐ Belgio - Data Protection Authority
- ☐ Bulgaria - Commission for Personal Data Protection
- ☐ Cipro - Office of the Commissioner for Personal Data Protection
- ☐ Croazia - Personal Data Protection Agency - AZOP
- ☐ Danimarca - Data Protection Agency
- ☐ Estonia - Data Protection Inspectorate
- ☐ Finlandia - Office of the Data Protection Ombudsman
- ☐ Francia - CNIL - National Commission for Informatics and Liberties
- ☐ Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI)
- ☐ Germania (Baden-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***0) 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

b. Esempi commentati di violazione

Esempio 1

Un supporto (cd/dvd/cassetta/ecc.) contenente un backup criptato con dati personali viene perso o rubato.

- Comunicazione al Garante: No.
- Comunicazione agli interessati: No.

Commento: Se i dati vengono crittografati con un algoritmo di ultima generazione, esistono dei backup dei dati e la chiave privata non è compromessa, non è necessario notificare la violazione. Tuttavia, se venisse compromessa anche successivamente, la notifica diverrà necessaria.

Esempio 2

Durante un cyber-attacco al sito web vengono rubati dati personali.

- Comunicazione al Garante: Sì, la notifica è necessaria in caso di potenziali danni ai soggetti interessati.
- Comunicazione agli interessati: Sì, la notifica dipende dalla natura dei dati violati e se è alto il livello di gravità dei potenziali danni.

Commento: Se il rischio non è elevato, consigliamo al titolare del trattamento di informare l'interessato, a seconda delle circostanze del caso. Ad esempio, la notifica potrebbe non essere necessaria in caso di violazione della riservatezza per una newsletter relativa ad un programma televisivo, mentre la notifica può essere richiesta se questa newsletter può portare a conoscenza del punto di vista politico del soggetto interessato.

Esempio 3

Una breve interruzione dell'alimentazione del call center del titolare del trattamento, che comporta l'impossibilità dei clienti di chiamare il titolare del trattamento e di accedere ai propri dati.

- Comunicazione al Garante: No.
- Comunicazione agli interessati: No.

Commento: Questa non è una violazione dei dati personali da notificare, ma solo un incidente di cui tenere nota ai sensi dell'art. 33, paragrafo 5.

Il titolare del trattamento dovrà redigere un apposito registro.

Esempio 4

Un titolare del trattamento subisce un attacco ransomware che causa la crittografia di tutti i dati. Nessun back-up è disponibile e i dati non possono essere ripristinati. Al momento dell'indagine, risulta evidente che l'unico scopo del ransomware era quello di crittografare i dati e che nessun altro malware veniva rilevato nel sistema.

- Comunicazione al Garante: Sì, la notifica è necessaria in caso di potenziali danni ai soggetti interessati, visto che questo attacco comporta una perdita di disponibilità dei dati.
- Comunicazione agli interessati: Sì, la notifica dipende dalla natura dei dati violati e dal possibile effetto della perdita di disponibilità dei dati, così come altre probabili conseguenze.

Commento: Se fosse disponibile un backup e se i dati potessero essere ripristinati in tempo utile, non sarebbe necessario segnalare al Garante o agli interessati poiché non ci sarebbe stata perdita permanente di disponibilità o riservatezza. Tuttavia, il Garante potrebbe considerare di verificare la conformità dei requisiti di sicurezza più ampi previsti dall'art. 32.

Esempio 5

Un interessato denuncia all'Ente una violazione di dati. Il soggetto ha ricevuto un documento contenente dati di qualcun altro.

Il titolare del trattamento intraprende una breve indagine (che va completata entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e se ciò è stato causato da un difetto sistemico che comporti il potenziale interessamento di altri soggetti.

- Comunicazione al Garante: No.
- Comunicazione agli interessati: Vengono notificati i soggetti interessati solo se esiste un rischio elevato ed è chiaro che altri soggetti non sono stati coinvolti.

Commento: Se, dopo ulteriori indagini, si è stabilito che sono interessati più soggetti, sarà necessario aggiornare il Garante ed il titolare del trattamento dovrà intraprendere, come azione supplementare, la notifica ad altri soggetti, in caso di loro rischio elevato.

Esempio 6

Una società di hosting web individua un errore nel codice che controlla l'accesso da parte degli utenti. L'anomalia comporta che qualunque utente possa accedere ai dettagli dell'account di qualsiasi altro utente.

- Comunicazione al Garante: Come responsabile del trattamento, la società di hosting web deve notificare tempestivamente al Garante quali suoi clienti (titolari del trattamento) sono coinvolti. Supponendo che la società di hosting web abbia effettuato una propria indagine, i titolari coinvolti dovrebbero essere ragionevolmente sicuri di sapere o meno di aver subito una violazione. Pertanto è da considerarsi "avvisato" una volta è stato oggetto di notifica dalla società di hosting (il responsabile del trattamento). Il titolare dovrà in seguito notificare la violazione all'autorità di vigilanza.
- Comunicazione agli interessati: Se non esiste un rischio elevato per i soggetti interessati, la notifica non è necessaria.

Commento: La società di hosting web (responsabile) deve considerare tutti gli altri obblighi di notifica (ad esempio, nell'ambito della direttiva NIS).

Se non vi è alcuna prova che questa vulnerabilità sia stata sfruttata da un particolare soggetto titolare, una notifica di violazione non può aver luogo ma è probabile che sia registrabile o che rientri nei casi di non conformità, ai sensi dell'art. 32.

Esempio 7

Un attacco informatico causa la non disponibilità dei registri medici in un ospedale per il periodo di 30 ore.

- Comunicazione al Garante: Sì, l'ospedale è tenuto a notificare al paziente che potrebbe verificarsi un alto rischio per il suo benessere e la sua privacy.
- Comunicazione agli interessati: Sì, la notifica è necessaria.

Esempio 8

I dati personali di 5000 studenti sono inviati per errore ad una mailing list sbagliata con più di 1000 destinatari.

- Comunicazione al Garante: Sì, la notifica è necessaria.
- Comunicazione agli interessati: Sì, la notifica è necessaria ai soggetti interessati, a seconda dell'ambito e tipo dei dati personali coinvolti e della gravità delle possibili conseguenze.

Esempio 9

Una e-mail di marketing diretto viene inviata ai destinatari nel campo "a:" o "cc:", consentendo così a ciascun destinatario di visualizzare l'indirizzo di posta elettronica di altri destinatari.

- Comunicazione al Garante: Sì, la notifica all'autorità di vigilanza può essere obbligatoria se è coinvolto un numero elevato di soggetti, se vengono rivelati dati sensibili (ad esempio una mailing list di un psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, la mail contiene le password iniziali).
- Comunicazione agli interessati: Sì, la notifica è necessaria ai soggetti interessati, a seconda del tipo dei dati personali coinvolti e della gravità delle possibili conseguenze.

Commento: La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili o se viene rivelato solo un numero ristretto di indirizzi di posta elettronica.

c. Modello di comunicazione agli interessati della violazione dei dati

G.mo Utente,

Secondo quanto prescritto dall'art. 34 del Regolamento Generale in materia di protezione dei dati personali RE (UE) 679/2016, L'Ente _____, titolare del trattamento, con la presente è a comunicarLe, l'intervenuta violazione dei Suoi dati personali (data breach) che si è verificata in data _____¹, alle ore _____²; data _____ alle ore _____;

NATURA DELLA VIOLAZIONE

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 li ha l'autore della violazione)
- ☐ _____

DISPOSITIVO OGGETTO DI VIOLAZIONE:

- ☐ Computer,
- ☐ Rete,
- ☐ Dispositivo mobile
- ☐ Strumento di backup
- ☐ Documento cartaceo
- ☐ _____

CHE TIPO DI DATI SONO OGGETTO DI VIOLAZIONE PER ESEMPIO:

- ☐ Dati anagrafici (nome, cognome, numero di telefono, e mail, CF, indirizzo ecc..)
- ☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica
- ☐ Dati personali idonei a rivelare le convinzioni religiose
- ☐ Dati personali idonei a rivelare filosofiche o di altro genere
- ☐ Dati personali idonei a rivelare le opinioni politiche

¹ A. Tra il ____ e il ____
B. In un tempo non ancora determinato
C. È possibile che sia ancora in corso

² Indicare l'ora se nota, altrimenti indicare l'ora in cui si viene a conoscenza della violazione.

- ☐ Dati personali idonei a rivelare l'adesione a partiti
- ☐ Dati personali idonei a rivelare sindacati,
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere religioso,
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere filosofico,
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere politico
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere sindacale
- ☐ Dati personali idonei a rivelare lo stato di salute
- ☐ Dati personali idonei a rivelare la vita sessuale
- ☐ Dati giudiziari
- ☐ Dati genetici
- ☐ Dati biometrici
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ _____

NOME E DEI DATI DI CONTATTO DEL DPO O UN ALTRO PUNTO DI CONTATTO PRESSO CUI OTTENERE PIÙ INFORMAZIONI:

DESCRIZIONE DELLE PROBABILI CONSEGUENZE DELLA VIOLAZIONE:

DESCRIZIONE DELLE MISURE ADOTTATE O DI CUI SI PROPONE L'ADOZIONE PER PORRE RIMEDIO ALLA VIOLAZIONE DEI DATI PERSONALI³

Scusandoci per quanto avvenuto rimaniamo a Sua disposizione per eventuali chiarimenti.

Firma Ente

³ e anche, se del caso, per attenuarne i possibili effetti negativi

d. Riepilogo adempimenti

Per schematizzare gli adempimenti ricollegabili alle valutazioni sopracitate si riporta la seguente tabella che può essere un supporto sebbene solo indicativo per la gestione dei Data Breach.

LIVELLO DI RISCHIO	ADEMPIMENTI
Rischio assente o basso	1. Compilazione del Registro delle Violazioni
Rischio medio	1. Compilazione del Registro delle Violazioni 2. Notifica al Garante
Rischio elevato	1. Compilazione del Registro delle Violazioni 2. Notifica al Garante 3. Comunicazione agli interessati