FONDAZIONE “BALDO IPPOLITA”

PROCEDURA IN CASO DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Regolamento UE n. 679/2016

Il Regolamento UE n. 679/2016 introduce l'obbligo di notifica di una violazione dei dati personali all'Autorità di Controllo. A partire dal 25 maggio 2018, tutti i Titolari del Trattamento dovranno notificare all'Autorità di Controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore** e comunque "senza ingiustificato ritardo".

La tempestiva comunicazione all'Autorità di Controllo deve avvenire solo se il Titolare del trattamento ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.

Da ciò consegue che la notifica all'Autorità di Controllo **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare. Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34.

Tutti i Titolari di trattamento dovranno in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all'Autorità di Controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

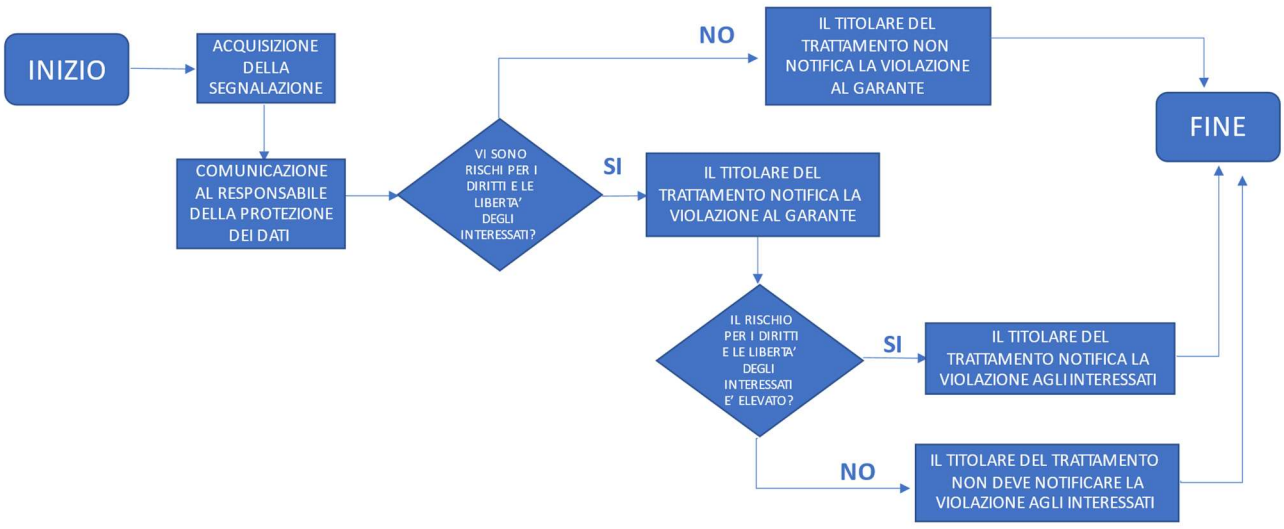
La mancata segnalazione di una violazione all'Autorità o agli interessati comporta ai sensi dell'articolo 83 del Regolamento UE una possibile sanzione applicabile al Titolare del trattamento.

I Titolari e i Responsabili del trattamento sono quindi incoraggiati a pianificare in anticipo e mettere in atto procedure specifiche per rilevare e contenere prontamente una violazione.

La **Fondazione Baldo Ippolita** presta particolare attenzione alla protezione dei dati personali al fine di evitare una violazione che potrebbe comprometterne la sicurezza.

Poiché il Titolare tratta dati personali dei dipendenti/consulenti/fornitori e dati personali e particolari degli ospiti residenti presso la Struttura, la compromissione di tali dati può comportare la violazione di diritti fondamentali degli interessati e un danno alla reputazione del Titolare del trattamento, oltre alla non conformità legislativa.

Le linee guida di seguito descritte definiscono le operazioni da seguire per garantire un approccio coerente ed efficace per la gestione degli incidenti relativi alla violazione dei dati e alla sicurezza delle informazioni, in ossequio allo schema sotto riportato.



DEFINIZIONI

Si definisce violazione di dato personale: "una violazione della sicurezza che porta alla distruzione, perdita, alterazione, divulgazione non autorizzata o accesso non autorizzato a dati personali trasmessi, archiviati o altrimenti elaborati".

Le principali tipologie di violazioni sono riconducibili a:

- **Violazione della riservatezza** - in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali.
- **Violazione della disponibilità** - in caso di perdita accidentale o non autorizzata di accesso o distruzione di dati personali.
- **Violazione dell'integrità** - in caso di alterazione non autorizzata o accidentale dei dati personali.

A seconda delle circostanze, una violazione può riguardare la riservatezza, la disponibilità o l'integrità dei dati personali allo stesso tempo, nonché qualsiasi combinazione di questi.

Se la mancanza di disponibilità temporanea di dati personali può comportare un rischio per i diritti e le libertà delle persone fisiche, il Titolare dovrà darne notifica. Questo dovrà essere valutato caso per caso.

Gli incidenti riguardanti la sicurezza e la loro definitiva risoluzione dovranno sempre essere adeguatamente documentati.

Gran parte delle problematiche relative alla sicurezza vengono scongiurate grazie ad una costante opera di prevenzione. Le attività su cui la **Fondazione Baldo Ippolita** focalizza la prevenzione sono sostanzialmente due, aspetto sociale ed aspetto tecnologico.

- Prevenzione sociale. La maggior parte degli incidenti di sicurezza derivano da un comportamento errato di chi opera con le strutture informatiche. Tali mancanze sono spesso dovute alla sottovalutazione dei reali pericoli esistenti. Occorre a tale scopo fare opera di sensibilizzazione verso le risorse più coinvolte e diffondere in maniera capillare policy mirate a stabilire regole e comportamenti "sicuri" da seguire.
- Prevenzione tecnologica. Per prevenzione tecnologica si intende la metodologia adottata per la manutenzione dell'ambiente tecnologico al fine di mantenere la "sicurezza" a livelli adeguati.

FINALITÀ E CAMPO DI APPLICAZIONE

Questa procedura si applica a tutto il personale del Titolare del trattamento. Pertanto, si applica anche al personale temporaneo, occasionale o di agenzia, i consulenti, i fornitori e i responsabili del trattamento dei dati che lavorano per conto del Titolare.

L'obiettivo di questa procedura è contenere eventuali violazioni, minimizzare il rischio associato alla violazione e considerare quale azione è necessaria per proteggere i dati personali e prevenire ulteriori violazioni.

SEGNALAZIONE INCIDENTI

Chiunque acceda, utilizzi o gestisca le informazioni della **Fondazione Baldo Ippolita** è responsabile di segnalare immediatamente violazioni alla sicurezza dei dati e incidenti informatici al Titolare del trattamento all'indirizzo fondazione@baldoippolita.it utilizzando il modello di cui all'Allegato A.

Se la violazione si verifica o viene scoperta al di fuori del normale orario di lavoro, deve essere segnalata non appena possibile.

Il rapporto includerà i dettagli completi e accurati dell'incidente, quando si è verificata la violazione (date e orari), chi lo segnala, se i dati si riferiscono a persone fisiche, la natura delle informazioni e il numero di persone coinvolte.

Tutto il personale deve essere consapevole che qualsiasi violazione della legge sulla protezione dei dati può comportare l'attivazione delle procedure disciplinari del Titolare del trattamento.

CONTENIMENTO E RECUPERO

Il Titolare del Trattamento determinerà innanzitutto se la violazione è ancora in corso. In tal caso, verranno presi immediatamente i provvedimenti appropriati per ridurre al minimo l'effetto della violazione.

Una valutazione iniziale verrà effettuata dal Titolare del Trattamento, in collaborazione con le funzioni coinvolte e competenti, per stabilire la gravità della violazione e chi assumerà l'iniziativa per indagare sulla violazione (ciò dipenderà dalla natura della violazione). In determinate situazioni potrà essere costituito un Team di investigazione e risposta agli incidenti al fine di agire in modo coordinato e tempestivo.

Il team sarà responsabile dell'analisi e della documentazione sulla effettiva portata della violazione della rete e delle risorse e di ogni danno da essa risultante ed elaborerà raccomandazioni per ogni eventuale azione correttiva.

Il Titolare del Trattamento stabilirà se c'è qualcosa che può essere fatto per recuperare eventuali perdite e limitare il danno che la violazione potrebbe causare. Stabilirà inoltre chi deve essere informato come parte del contenimento iniziale e informerà se necessario la polizia postale e le Autorità.

INDAGINE E VALUTAZIONE DEL RISCHIO

Il Titolare del Trattamento effettuerà un'indagine immediatamente e ovunque possibile entro 24 ore dalla scoperta / segnalazione della violazione.

Il Titolare del Trattamento esaminerà la violazione e valuterà i rischi ad essa associati, ad esempio le potenziali conseguenze negative per gli individui e quanto gravi o sostanziali siano.

L'indagine dovrà tenere conto di quanto segue:

- il tipo di dati coinvolti;
- la "sensibilità" ai fini privacy;
- le protezioni che sono in atto (ad es. Log, Crittografie, etc.);
- cosa è successo ai dati, cosa è stato perso o rubato;
- se i dati potrebbero essere utilizzati in modo illegale o inappropriato;
- chi sono gli individui, numero di persone coinvolte e potenziali effetti su tali soggetti interessati;
- se ci sono conseguenze più ampie sulla violazione.

In questa fase sono prese in esame anche le informazioni contenute nel Registro dei Trattamenti e nel Documento di Valutazione d'Impatto sulla protezione dei dati inerente rischi e misure.

Al termine dell'indagine e delle eventuali notifiche, il Titolare del trattamento compilerà una scheda contenente tutte le informazioni/valutazioni in merito alla violazione dei dati, utilizzando il modello di cui all'Allegato B.

NOTIFICA

Il Titolare del trattamento in accordo con il Responsabile IT determinerà, terminata la fase investigativa, chi deve essere informato della violazione.

Ogni incidente sarà valutato caso per caso; tuttavia, sarà necessario considerare quanto segue:

- Se procedere con la notifica all'Autorità Garante;
- Se esistono requisiti di notifica legale / contrattuale;

L'articolo 33, paragrafo 1 stabilisce che:

"in caso di violazione dei dati personali, il titolare del trattamento procede senza indebiti ritardi e, ove possibile, entro 72 ore dopo averne preso atto, notifica la violazione dei dati personali all'autorità di controllo competente ai sensi dell'articolo 55, a meno che è improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Se la notifica all'autorità di controllo non viene effettuata entro 72 ore, è accompagnata dai motivi del ritardo".

I Responsabili del Trattamento che sono venuti a conoscenza della violazione sono tenuti ad informare il Titolare senza ingiustificato ritardo e a collaborare con esso.

Questo è importante per aiutare il Titolare del trattamento a soddisfare l'obbligo di notifica al Garante entro 72 ore.

Il Titolare del trattamento deve prendere in considerazione, inoltre, l'eventuale notifica a terzi come la polizia, gli assicuratori, le società bancarie e i sindacati.

Le informazioni da notificare all'Autorità di Controllo sono:

- la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati e le categorie e il numero approssimativo di record di dati personali interessati;
- il nome e i dettagli di contatto del Responsabile della Protezione dei Dati o di altri punti di contatto in cui possono essere ottenute maggiori informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o proposte per essere adottate dal Responsabile del Trattamento per affrontare la violazione dei dati personali comprese, se del caso, misure per mitigarne gli eventuali effetti negativi.

La notifica all'Autorità avverrà mediante l'invio di un form da compilare on line all'indirizzo http://servizi.gpdp.it/databreach/s/ e contenente tutte le richieste indicate nell'Allegato C).

In alcuni casi, oltre a notificare al Garante, il Titolare del trattamento è tenuto a comunicare una violazione agli individui interessati. Tale comunicazione avverrà utilizzando il modello allegato alla presente procedura (Allegato D)

L'articolo 34, paragrafo 1, afferma:

"*Quando la violazione dei dati personali può comportare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione dei dati personali all'interessato senza indebiti ritardi*."

Secondo questa disposizione, il Titolare del trattamento dovrebbe fornire agli interessati almeno le seguenti informazioni:

- una descrizione della natura della violazione;
- il nome e i dettagli di contatto del Responsabile della Protezione dei Dati o di altri punti di contatto;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o proposte da adottare dal responsabile del trattamento per affrontare la violazione comprese, eventualmente, misure per mitigarne gli eventuali effetti negativi.

L'articolo 34, paragrafo 3 del Regolamento stabilisce tre condizioni che, se soddisfatte, non richiedono la notifica ai singoli in caso di violazione, di seguito brevemente descritte:

- Il Titolare del trattamento ha applicato misure tecniche e organizzative adeguate a proteggere i dati personali prima della violazione, in particolare quelle misure che rendono i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi.
- Immediatamente dopo una violazione, il Titolare del trattamento ha adottato misure per garantire che non sia più probabile che si concretizzi l'alto rischio posto ai diritti e alle libertà delle persone.
- Contattare le persone comporterebbe uno sforzo sproporzionato. In caso di sforzi sproporzionati, potrebbero anche essere previste disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta, che potrebbero rivelarsi utili per le persone che potrebbero essere interessate da una violazione.

VALUTAZIONE E RISPOSTA

Una volta che l'incidente iniziale è stato contenuto, il Titolare del trattamento effettuerà una revisione completa delle cause della violazione, verificando l'efficacia della risposta e valutando l'eventuale necessità di modificare sistemi, politiche e procedure.

L'analisi prenderà in considerazione:

- Dove e come vengono conservati i dati personali, dove e come sono archiviati;
- Dove risiedono i maggiori rischi e individuerà eventuali ulteriori punti deboli all'interno delle misure esistenti;
- se i metodi di trasmissione sono sicuri e se vi è la condivisione della quantità minima di dati;
- Identificazione dei punti deboli all'interno delle misure di sicurezza esistenti;

- Consapevolezza del personale.

DOCUMENTARE LA VIOLAZIONE

Indipendentemente dal fatto che una violazione debba o meno essere notificata all'Autorità di Controllo, il Titolare del trattamento deve conservare la documentazione di tutte le violazioni. Gli incidenti e le violazioni sono registrati in apposito Registro degli Incidenti e Violazioni (Allegato E).

Allegati:

Allegato A: Modello di Segnalazione dell'evento

Allegato B: Scheda della violazione

Allegato C: Modello di notifica delle violazioni dei dati

Allegato D: Modello di comunicazione all'interessato

Allegato E: Registro violazioni dei dati