

# Gestione interna di un **Data Breach**

## **1. INFORMAZIONI GENERALI**

Il presente documento descrive il processo adottato per la gestione delle violazioni di sicurezza che comportano gravi rischi dei diritti e delle libertà degli Interessati, le cui informazioni personali sono trattate e custodite presso i sistemi IT e presso i locali del Titolare del trattamento.

Il Data Breach è una violazione della sicurezza, che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione, accesso, copia o consultazione non autorizzate di dati personali trasmessi, conservati o comunque trattati. Ciò può avvenire a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB, etc.) o per la sottrazione di documenti con dati personali (furto, etc.).

## 2. RUOLI E RESPONSABILITÀ

<b>Ragione sociale:</b>	CROCE ROSSA ITALIANA - COMITATO LOCALE DI TRENTO ODV
<b>Sede legale:</b>	Via della Croce, 63/A - Ravina 38123 Trento (TN)
<b>P.iva.:</b>	02360810226
<b>C.F.:</b>	02360810226
<b>Codice ATECO (2007):</b>	94.99.9

<b>Responsabile Protezione dei dati ex art 39 del GDPR</b>	Giovanni Poletto
--	------------------

## 3. SCOPO E AMBITO DI APPLICAZIONE

La procedura ha l'obiettivo di definire un processo chiaro e uniforme per la gestione delle violazioni dei dati personali, garantendo la conformità al GDPR (Regolamento UE 2016/679) e minimizzando i rischi per i diritti e le libertà degli interessati. Si applica a tutti i soggetti interni ed esterni che trattano dati personali per conto del Titolare del trattamento.

## 4. REVISIONI

Di seguito viene riportata una tabella dove è indicato lo stato del documento, con indicazione della prima emissione e delle varie revisioni del documento stesso.

N° emissione	N° revisione	Data	Note
1	0	2018	Prima Emissione del documento
2	0	29/04/2025	<b>Emissione nuovo documento</b>

## 5. CHE COSA È UN DATA BREACH

Una violazione di dati personali o qualsiasi infrazione relativa alla sicurezza degli stessi che comporti - 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 dal Titolare del trattamento. Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

## 6. LIVELLI DI DATA BREACH (BASATI SULLA GRAVITÀ)

Viene definita una classificazione a tre livelli *basata sulla gravità* per facilitare la risposta proporzionata e adeguata a ciascuna violazione:

### 1. Livello 1 (Basso impatto):

Violazione che *probabilmente* non comporta rischi significativi per i diritti e le libertà degli interessati. Tipicamente coinvolge dati non sensibili, con limitate possibilità di identificazione e minimi danni potenziali. Esempi: perdita di dati di contatto non critici, accessi non autorizzati a informazioni pubbliche.

### 2. Livello 2 (Medio impatto):

Violazione che *potrebbe* comportare rischi per i diritti e le libertà degli interessati. Coinvolge dati sensibili, con una moderata possibilità di identificazione e possibili danni reputazionali o finanziari. Esempi: accesso non autorizzato a dati sanitari non critici, compromissione di credenziali di accesso a sistemi secondari.

### 3. Livello 3 (Alto impatto):

Violazione che *probabilmente* comporta un alto rischio per i diritti e le libertà degli interessati. Coinvolge dati particolarmente sensibili (dati biometrici, orientamento sessuale, dati finanziari completi), con alta possibilità di identificazione e gravi danni potenziali (furto d'identità, frode finanziaria, discriminazione). Esempi: attacco ransomware che compromette dati sanitari, accesso non autorizzato a database con informazioni finanziarie.

## 7. FASI OPERATIVE

### Step 1: Identificazione e indagine preliminare

- 1. Segnalazione dell'incidente:**  
Utilizzare il modulo di comunicazione interna (Allegato A) per notificare il data breach al Titolare del trattamento e al RPD/DPO.
- 2. Valutazione iniziale:**  
Analizzare:
  - Data e ora di scoperta della violazione.
  - Natura dell'incidente e dati coinvolti.
  - Numero approssimativo degli interessati (per dare un'idea della *scala* potenziale, ma non è il fattore decisivo).
  - Azioni già intraprese.
- 3. Coinvolgimento del RPD/DPO:**  
Se necessario, attivare il supporto del Responsabile IT e del Responsabile della Sicurezza.
- 4. Registrazione sul registro delle non conformità:**
- 5.** tutti gli incidenti vanno registrati, indipendentemente dal livello di rischio.

### Step 2: Contenimento, recupero e valutazione del rischio

- 1. Azioni immediate:**
  - Isolare sistemi compromessi.
  - Recuperare dati da backup.
  - Cambiare credenziali d'accesso compromesse.
- 2. Valutazione del rischio (Allegato B – o con altri metodi):**
- 3.** Determinare il livello del data breach (Livello 1, 2 o 3) *basandosi sulla gravità potenziale* e valutare la violazione considerando:
  - Natura, sensibilità e volume dei dati personali coinvolti (art. 32 GDPR).
  - Facilità di identificazione degli interessati.
  - Probabilità di danni futuri (es. furto d'identità, frode finanziaria).
  - Misure di sicurezza tecniche e organizzative già in atto.
- 4. Decisione su notifiche/comunicazioni:**  
Stabilire se notificare l'Autorità Garante (art. 33 GDPR) e/o comunicare agli interessati (art. 34 GDPR). Questa decisione deve essere *basata sulla valutazione della probabilità e della gravità del rischio per gli interessati*.

### Step 3: Notifica all'Autorità Garante (Art. 33 GDPR)

- 1. Obbligo di notifica:**  
Se la valutazione del rischio indica che la violazione *può* comportare un rischio per i diritti e le libertà delle persone fisiche, notificare l'Autorità Garante entro 72 ore dalla scoperta dell'incidente (art. 33, par. 1 GDPR).
- 2. Contenuto della notifica (art. 33, par. 3 GDPR):**
  - Natura della violazione.
  - Categorie e numero approssimativo degli interessati (se possibile).
  - Categorie e numero approssimativo dei dati personali (se possibile).
  - Nome e dati di contatto del RPD/DPO.
  - Probabili conseguenze della violazione.
  - Misure adottate o proposte per porre rimedio alla violazione.
- 3. Eccezioni:**  
La notifica all'Autorità Garante non è richiesta se è *improbabile* che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche (art. 33, par. 5 GDPR). *Documentare accuratamente la motivazione per cui non si è notificata la violazione.*

#### Step 4: Comunicazione agli interessati (Art. 34 GDPR)

1. **Obbligo di comunicazione:** Se la valutazione del rischio indica che la violazione *presenta un rischio elevato* per i diritti e le libertà delle persone fisiche, comunicare la violazione agli interessati senza ingiustificato ritardo (art. 34, par. 1 GDPR).
2. **Contenuto della comunicazione (art. 34, par. 2 GDPR):**
  - Descrizione chiara e semplice della natura della violazione.
  - Nome e dati di contatto del RPD/DPO.
  - Raccomandazioni per proteggere gli interessati da potenziali danni (es. monitoraggio degli estratti conto bancari, cambio password).
3. **Eccezioni (art. 34, par. 3 GDPR):**

La comunicazione agli interessati non è richiesta se:

  - Sono state adottate misure tecniche e organizzative adeguate per rendere i dati incomprensibili a persone non autorizzate (es. cifratura).
  - Sono state adottate misure successive per garantire che il rischio elevato non si concretizzi.
  - La comunicazione richiederebbe sforzi sproporzionati (in tal caso, è sufficiente una comunicazione pubblica).

#### Step 5: Documentazione della violazione (Art. 33, par. 5 GDPR)

1. Registrare l'incidente nel Registro delle attività di trattamento (RAT).
2. Documentare tutte le azioni intraprese, inclusi i moduli Allegato A e B, la valutazione del rischio (con la motivazione del livello attribuito), le notifiche all'Autorità Garante (se effettuate), e le comunicazioni agli interessati (se effettuate).
3. Mantenere la documentazione per un periodo di tempo adeguato (es. 5 anni).
4. **Analisi post-incidente**
  - Condurre una root cause analysis per identificare le cause dell'incidente.
  - Aggiornare le misure di sicurezza tecniche e organizzative per prevenire futuri data breach.
  - Valutare l'efficacia delle procedure di risposta agli incidenti e apportare eventuali miglioramenti.
5. **Formazione e sensibilizzazione**
  - Formare regolarmente il personale sulla procedura di gestione dei data breach e sulle misure di sicurezza da adottare.
  - Simulare scenari di violazioni per migliorare la reattività.
  - Sensibilizzare il personale sui rischi legati alla sicurezza dei dati personali.

#### Allegati

- Allegato A – Modulo di comunicazione interna di Data Breach
- Allegato B – Modulo di valutazione del rischio connesso al Data Breach (non vincolante)

## Allegato A – Modulo di comunicazione interna di Data Breach

Questo modulo serve a raccogliere informazioni preliminari sull'incidente, permettendo al Titolare del trattamento o al suo delegato di condurre una valutazione iniziale. Include:

- Data di scoperta della violazione (tempestività).
- Soggetto che ha rilevato la violazione.
- Descrizione dell'incidente, con dettagli sulla natura della violazione e sui dati coinvolti.
- Categorie e numero approssimativo degli interessati colpiti.
- Azioni già intraprese per contenere o mitigare l'impatto.

## Allegato B – Modulo di valutazione del rischio connesso al Data Breach

Questo modulo è utilizzato per determinare la gravità della violazione e valutare il rischio per i diritti e le libertà degli interessati. Include:

- Analisi del rischio basata su criteri come il tipo di dati coinvolti, il volume dei dati esposti e la probabilità di danno.
- Indicazioni per stabilire se è necessario notificare l'Autorità Garante o comunicare agli interessati.
- Supporto decisionale per distinguere tra rischio semplice (notifica all'Autorità) e rischio elevato (comunicazione agli interessati).

Nota:

L' **Allegato B** offre esclusivamente un metodo di valutazione. Qualora necessario, potranno essere utilizzati altri approcci, come ad esempio il metodo descritto nelle linee guida dell'ENISA (Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione) o il sistema messo a disposizione dal Garante per la protezione dei dati personali.

### Allegato A: Modulo di comunicazione interna di Data Breach

Campo	Descrizione
Informazioni generali su DB	
Data e ora della segnalazione	
Soggetto che segnala	[Nome, Cognome, Dipartimento/Funzione]
Dettagli dell'incidente	
Data e ora presunte dell'incidente	[Data e ora]
Luogo dell'incidente	[Ubicazione fisica o sistema informatico coinvolto]
Descrizione dettagliata dell'incidente	[Fornire una descrizione accurata di cosa è successo, come è stato scoperto e quali sistemi/dati sono coinvolti]
Tipo di violazione	[Es. accesso non autorizzato, perdita/furto dispositivo, errore umano, attacco malware]
Dati coinvolti	
Tipi di dati personali interessati	[Es. nome, indirizzo, email, dati finanziari, dati sanitari, ecc.]
Volume approssimativo dei dati	[Numero stimato di record o persone coinvolte]
Categorie di interessati coinvolti	[Es. clienti, dipendenti, fornitori, ecc.]
Azioni intraprese	
Misure immediate adottate	[Descrivere le azioni immediate intraprese per contenere la violazione o mitigarne l'impatto (es. isolamento sistemi, cambio password)]
Ulteriori azioni raccomandate	[Suggerimenti per ulteriori azioni da intraprendere]
Valutazione preliminare	
Impatto potenziale stimato	[Valutazione preliminare dell'impatto sulla privacy degli interessati e sull'organizzazione]
Richiesta di supporto	[Indicare se è necessario supporto IT, legale o di comunicazione]
Nome e firma del segnalante	[Nome e firma]
Nome e firma del DPO	[Nome e firma]

## Allegato B: Modulo di valutazione del rischio connesso al Data Breach

La presente tabella non ha valore vincolante per la valutazione del Data Breach, ma rappresenta uno strumento utile per guidare una corretta e ponderata valutazione del caso.

Critero di valutazione	Basso (1)	Medio (2)	Alto (3)	Punteggio
Tipo di dati	Dati non sensibili (es. informazioni di contatto generiche)	Dati sensibili (es. dati personali identificativi, informazioni finanziarie limitate)	Dati altamente sensibili (es. dati sanitari, dati biometrici, informazioni finanziarie complete)	
Volume dei dati	Numero limitato di record (meno di 100)	Numero moderato di record (tra 100 e 1.000)	Numero elevato di record (oltre 1.000)	
Facilità di identificazione	Dati anonimizzati o pseudonimizzati con difficoltà di re-identificazione	Dati pseudonimizzati con possibilità di re-identificazione	Dati identificativi diretti (es. nome, indirizzo, codice fiscale)	
Probabilità di danno	Bassa probabilità di danni per gli interessati (es. nessun rischio finanziario o reputazionale)	Moderata probabilità di danni (es. potenziale rischio di furto d'identità, danni reputazionali limitati)	Alta probabilità di danni significativi (es. rischio elevato di furto d'identità, danni reputazionali gravi, conseguenze finanziarie rilevanti)	
Misure di sicurezza implementate	Misure di sicurezza adeguate e tempestive	Misure di sicurezza parzialmente adeguate o non completamente aggiornate	Assenza o insufficienza di misure di sicurezza adeguate	
Punteggio totale	[Somma dei punteggi per ciascun criterio]			
Valutazione del rischio	Basso: (5-8) - Rischio minimo, monitoraggio continuo	Medio: (9-12) - Rischio moderato, valutare la notifica all'Autorità Garante	Alto: (13-15) - Rischio elevato, notifica all'Autorità Garante e comunicazione agli interessati	
Decisioni				
Necessità di notifica al Garante	Sì No			
Necessità di comunicazione agli interessati	Sì No			
Azioni correttive da intraprendere	[Elenco delle azioni correttive da intraprendere per mitigare il rischio e prevenire future violazioni]			

Istruzioni:

1. Compilare entrambi i moduli in modo accurato e completo.
2. Utilizzare le informazioni raccolte per valutare il rischio e prendere decisioni informate sulla gestione del data breach.
3. Conservare i moduli compilati come parte della documentazione dell'incidente.