



## **Procedura “Data breach”**

*Violazione dei dati personali dell’Interessato*

### **PROCEDURA E DIARIO DEI DATA BREACH** *(Violazione dei dati personali)*

**Definizione di “data breach”:** Una violazione di sicurezza che comporta, accidentalmente o in modo illecito:

- La distruzione
- La perdita
- La modifica
- La divulgazione non autorizzata
- L’accesso ai dati personali trasmessi, conservati o comunque trattati.

Una violazione di dati personali può compromettere la riservatezza, l’integrità o la disponibilità dei dati personali.

Alcuni possibili esempi:

- L’accesso o l’acquisizione dei dati da parte di terzi non autorizzati;
- Il furto o la perdita di dispositivi informatici contenenti dati personali;
- La deliberata alterazione dei dati personali
- L’impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, *malware*, ecc
- La perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi od altre calamità;
- La divulgazione non autorizzata dei dati personali.

(Fonte: <https://www.garantepriacy.it/regolamentoue/databreach>)

Qualsiasi evento che rientri nelle casistiche sopra enunciate, in qualunque modo posto a conoscenza del Centro Chirone, deve far partire, nell’immediatezza (del fatto o dell’avvenuta conoscenza) la **procedura data breach**.

1. Chiunque accerti o venga a conoscenza di una violazione subita dal Centro, ne avverte immediatamente, per telefono e per iscritto (a mezzo e-mail) il Titolare del trattamento.
2. Lo stesso provvederà alla redazione della scheda interna di rilevazione, allegata alla presente procedura nonché nel successivo aggiornamento del **“diario delle violazioni”**.
3. Il Titolare attiva il coordinamento fra le funzioni o i soggetti ritenuti utili e necessari, anche ai fini di valutare l’evento, le cause, le conseguenze e le possibili ricadute sui diritti e le libertà degli Interessati, le contromisure immediate per l’evento e la programmazione di contromisure future, idonee a minimizzare o scongiurare eventi simili.
4. Ad esito del coordinamento, di cui deve rimanere **un verbale scritto da lasciare a disposizione anche dell’Autorità di controllo**, si valuterà se:
  - a. Lasciare il tutto come accadimento interno senza ulteriori seguiti verso l’esterno;
  - b. Notiziare l’Autorità Garante entro 72 ore da quando si è venuti a conoscenza dei fatti;
  - c. Informare anche gli Interessati, senza ingiustificato ritardo, circa il fatto e le possibili conseguenze.



## **Procedura “Data breach”**

*Violazione dei dati personali dell'Interessato*

- 5. Il diario delle violazioni è costituito da un prospetto generale riassuntivo, dalle singole schede interne di rilevazione nonché dai verbali di coordinamento. Il Diario è custodito a cura del titolare e posto a disposizione dell'Autorità Garante.**

## **NORMATIVA DI RIFERIMENTO (G.D.P.R.)**

### **Articolo 33 Notifica di una violazione dei dati personali all'autorità di controllo**

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
  - a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
  - b) 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;
  - c) descrivere le probabili conseguenze della violazione dei dati personali;
  - d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

### **Articolo 34 Comunicazione di una violazione dei dati personali all'interessato**

1. 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 comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:



## **Procedura “Data breach”**

*Violazione dei dati personali dell’Interessato*

- a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
- c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all’interessato la violazione dei dati personali, l’autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

## **COMUNICAZIONE ALL’AUTORITA’ GARANTE**

### **COMUNICAZIONE DI VIOLAZIONE DI DATI PERSONALI DELL’INTERESSATO**

La procedura di comunicazione dei *data breach*, all’Autorità Garante, è prevista esclusivamente in modalità *on line*, accedendo al sito *web* dell’Autorità, alla pagina <https://servizi.gdpd.it/databreach/s/>

Ai fini della miglior valutazione dell’evento e delle sue conseguenze, il sito propone una procedura di autovalutazione, definita “*self assesment*” reperibile all’indirizzo <https://servizi.gdpd.it/databreach/s/self-assessment>

Pur in presenza di una procedura digitalizzata, per la quale è necessario autenticarsi mediante firma digitale (a breve anche mediante SPID ed altri sistemi non disponibili alla data di redazione della presente procedura), si ritiene comunque utile proporre uno schema degli elementi richiesti, al fine di arrivare preparati alla compilazione evitando errori o perdite di tempo.

Le informazioni richieste sono le seguenti:

#### **1. MOMENTO DELL’AVVENUTA CONOSCENZA:**

Giorno	Numero	Mese	Anno	Ora	Minuto

CONTATTI NECESSARI	NOME E COGNOME	TELEFONO	POSTA ELETTRONICA
RESPONS. PROTEZIONE DATI			
ALTRO PUNTO DI CONTATTO			

#### **2. MOTIVO DELL’EVENTUALE RITARDO NELLA COMUNICAZIONE: (specificare).**



## **Procedura “Data breach”**

*Violazione dei dati personali dell’Interessato*

**3. NATURA DELLA VIOLAZIONE:** *descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione).*

**4. PROBABILI CONSEGUENZE DELLA VIOLAZIONE:** *descrivere le probabili conseguenze della violazione.*

**5. MISURE ADOTTATE O PROPOSTE DA PARTE DEL TITOLARE DEL TRATTAMENTO:** *descrivere le misure adottate o di cui si propone l’adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi).*

**6. EVENTUALI INFORMAZIONI CHE SARANNO FORNITE SUCCESSIVAMENTE.**

\*\*\*\*\*

Allegato: Scheda di rilevazione