# Procedura per la gestione delle violazioni di dati personali (*data breach*)

5 Settembre 2019

Questo documento descrive schematicamente la procedura da seguire per la gestione di un *data breach* e presuppone la conoscenza di quanto scritto nel documento *La violazione dei dati personali (data breach)*, pubblicato su https://dpo.infn.it/documenti-dpo/.

### 1. Rilevazione e segnalazione data breach

Chiunque rilevi o sospetti un data breach è tenuto a darne segnalazione immediata, preferibilmente per e-mail, al Direttore[1], al Responsabile del Servizio Calcolo[2] e al Referente locale del DPO[3].

### 2. Raccolta delle informazioni sulla violazione

Il Direttore, ricevuta la segnalazione, ove lo ritenga necessario e sentiti il Responsabile del Servizio Calcolo e il Referente locale del DPO, incarica coloro che per ruolo e competenze possano effettuare con la **massima celerità** un approfondimento circa la violazione segnalata, raccogliendo informazioni e verificandone la fondatezza.

L'esito delle attività di approfondimento è comunicato al Direttore **senza ritardo**. Se la verifica ha evidenziato un'effettiva violazione, da questa comunicazione decorrono le **72 ore** per l'eventuale notifica all'Autorità Garante per la protezione dei dati personali.

---

1 In tutto questo documento, per "Direttore", a seconda dei casi, si intende la Direttrice o il Direttore della Struttura, dell'articolazione dell'Amministrazione Centrale, la | il Responsabile del Servizio di Presidenza o dell'Ufficio Comunicazione.

2 Per "Responsabile Servizio Calcolo" si intende il responsabile delle infrastrutture informatiche della sede.

3 Per questo tipo di segnalazioni si suggerisce una *mailing list* locale, **ampiamente pubblicizzata.**

### 3. Valutazione di impatto e individuazione delle azioni correttive

Il Direttore, insieme al Responsabile del Servizio Calcolo se la violazione è di tipo informatico, al referente locale del DPO e, se lo ritiene necessario, al DPO, ne valuta l'impatto e individua le azioni correttive per ridurne gli effetti negativi e evitarne la ripetizione[4], dando disposizioni per la loro adozione.

### 4. Eventuale notifica della violazione

Se il data breach **comporta un rischio** per i diritti e le libertà delle persone fisiche, il Direttore, senza ritardo e comunque entro 72 ore da quando ne è venuto a conoscenza (**punto 2**), notifica la violazione al Garante, al DPO e al Direttore Generale utilizzando il modulo disponibile su https://dpo.infn.it/documenti-dpo/[5]. In caso contrario si passa al **punto 7**.

Se l'incidente è particolarmente complesso, il Direttore effettua la notifica con i dati disponibili all'esito del primo approfondimento. In questo caso la notifica conterrà la segnalazione che le informazioni trasmesse non sono complete e che seguiranno ulteriori fasi di notifica, effettuate sempre secondo le indicazioni qui contenute.

### 5. Comunicazione agli interessati

Se la violazione è suscettibile di presentare un **rischio elevato**[6] per i diritti e le libertà delle persone fisiche, il Direttore comunica agli interessati le eventuali conseguenze della violazione e le misure da adottare per la riduzione delle conseguenze e del rischio. La comunicazione agli interessati dovrà essere effettuata in modo esclusivo, cioè non insieme ad altre notizie di diverso contenuto e diretta a ciascuno di essi. Se la comunicazione diretta comportasse uno sforzo sproporzionato, potrà essere effettuata mediante pubblicazione in un sito accessibile agli interessati.

### 6. Recepimento della eventuale risposta del Garante

Il Direttore comunica a tutti i soggetti coinvolti dalla violazione le disposizioni per l'attuazione delle misure correttive eventualmente indicate dal Garante.

---

4 Per i criteri da seguire per la valutazione del rischio si rimanda ai documenti *La violazione dei dati personali (data breach)* e *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679* entrambi reperibili su https://dpo.infn.it/

5 Cfr. il paragrafo Note per la compilazione della notifica.

6 Si parla di **rischio elevato** quando la violazione può arrecare danni fisici, materiali o immateriali per coloro i cui dati sono stati violati. Tra questi la discriminazione, il furto d'identità, la frode, le perdite finanziarie o il danno alla reputazione. A maggior ragione se la violazione coinvolge dati personali che rivelano l'origine etnica, l'opinione politica, religiosa o filosofica o includono dati genetici o dati sulla salute o l'orientamento sessuale o informazioni connesse alla commissione di reati e conseguenti sanzioni o misure di sicurezza.

### 7. Notifica nel caso di assenza di rischio per i diritti delle persone

Se il data breach **non comporta un rischio** per i diritti e le libertà delle persone fisiche, il Direttore comunica solo al DPO e al Direttore Generale il risultato della valutazione di impatto e le eventuali azioni da intraprendere (**punto 3**), sempre utilizzando il modulo disponibile all'indirizzo https://dpo.infn.it/documenti-dpo/, e indicando il motivo della mancata notifica al Garante.

### 8. Notifica al CERT PA

Il Direttore notifica la violazione allo CSIRT di riferimento[7] e al CERT-PA, allegando il documento con la descrizione dell'implementazione delle misure minime AgID nella Struttura.

Se la violazione evidenzia condotte penalmente rilevanti, il Direttore provvede alla denuncia all'Autorità Giudiziaria.

7 INFN CSIRT e/o GARR-CERT.

# Note per la compilazione della notifica

La notifica deve essere **firmata digitalmente** e inviata a:

- Autorità Garante per la protezione dei dati personali:
  **protocollo@pec.gpdp.it**[8]
- Direttore Generale INFN:
  **amm.ne.centrale@pec.infn.it**
- DPO INFN:
  **dpo@infn.it**

Se la notifica non viene inviata al Garante, il documento di accompagnamento deve indicare il motivo per cui si è ritenuto di non inviarla.

### Sez. A

#### Funzione rivestita

Direttrice | Direttore della Struttura / Direttrice | Direttore dell'articolazione dell'Amministrazione Centrale / Responsabile del Servizio di Presidenza / Responsabile dell'Ufficio Comunicazione

8 Solamente se la violazione comporta un rischio per i diritti e le libertà delle persone fisiche.

Procedura per la gestione delle violazioni di dati personali (5/9/19)