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

1 settembre 2021

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 del data breach

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

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 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, dando disposizioni per la loro adozione.

Per un aiuto nella valutazione della gravità della violazione e nell'individuazione delle azioni da intraprendere si rimanda alla procedura di autovalutazione raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/self-assessment.

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 tramite la procedura telematica raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/, e invia i documenti che riceverà - i dati trasmessi, il numero di fascicolo creato e pin - al DPO e al Direttore Generale. 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 comunicazione 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 per i diritti e le libertà delle persone fisiche**, il Direttore comunica agli interessati le eventuali conseguenze della violazione e le misure che verranno adottate 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.

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**) riempiendo e **firmando digitalmente** il modulo *NOTIFICA IN-*

TERNA DI VIOLAZIONE DI DATI PERSONALI, disponibile all'indirizzo https://dpo.infn.it/documenti-dpo/violazione-dati-personali-e-relativi-modelli/.

8. Notifica all'INFN CSIRT e eventuale denuncia all'Autorità Giudiziaria

Il Direttore notifica la violazione all'INFN CSIRT utilizzando la procedura descritta in https://www.csirt.infn.it/p.html.

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

Note per la compilazione della notifica al Garante

A) Dati del soggetto che effettua la notifica

Il sottoscritto ….

nella sua qualità di

- delegato del rappresentante legale

  Cognome **Zoccoli** Nome **Antonio**

B) Tipo di notifica

La notifica viene effettuata:

- ai sensi dell'art. 33 del RGPD

C) Titolare del trattamento

1. **Il titolare del trattamento è**
   - 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)
2. **Dati del Titolare del trattamento**

   Denominazione: **Istituto Nazionale di Fisica Nucleare**
   Codice Fiscale/P.IVA: **84001850589**
   Stato: **Italia**
   Comune: **Frascati** CAP: **00044**
   Provincia: **Roma**
   Indirizzo: **Via E. Fermi, 54**
   Telefono: **06 94032477**
   E-mail: **legale@lnf.infn.it**
   PEC: **amm.ne.centrale@pec.infn.it**

D) Dati di contatto per informazioni relative alla violazione

1. **Responsabile della protezione dei dati**
   - i cui dati di contatto sono stati già comunicati con la comunicazione protocollo n. **RPD.0002039.22/05/2018**

Data breach: obblighi di notifica