ISTITUTO NAZIONALE DI GEOFISICA E VULCANOLOGIA

il Direttore

Istituto Nazionale di Geofisica
e Vulcanologia
AOO INGV
Protocollo Generale - U
N 0016274
del 13/11/2019

Gestione WEB

Al Responsabile per la Protezione dei Dati
Ai Componenti Ufficio DPO
Ai Componenti del GdL a supporto Ufficio DPO
Ai Direttori di Dipartimento
Ai Direttori di Sezione
Al Direttore delle Direzioni Centrali
Al Responsabile della Prevenzione della Corruzione e della Trasparenza
Ai Responsabili dei Centri Servizi
Al Settore Affari Legali e Contenzioso
Al Capo dell'Ufficio Procedimenti Disciplinari
Alle Segreterie delle Sezioni
Ai Responsabili dei Servizi Amministrativi delle Sezioni
Al Personale dell'Amministrazione Centrale

Oggetto: Pubblicità atti

Si notifica in copia l'allegata Delibera n. 203/2019 del 11/10/2019 – Allegato G al Verbale n. 08/2019 concernente: Procedura di gestione delle violazioni dei dati personali *(data breach)* ai sensi degli artt. 33 e 34 del Regolamento UE 2016/679.

Dott. Giovanni TORRE

DIREZIONE CENTRALE
AFFARI DEL PERSONALE

Via di Vigna Murata, 605 | 00143 Roma| Italia | Tel.: +39 39.0651860448 | Fax: +39.0651860576
direzione.centrale1@ingv.it | aoo.roma@pec.ingv.it | www.ingv.it

Delibera n. 203/2019
Allegato G al Verbale n. 08/2019
Oggetto: Procedura di gestione delle violazioni dei dati personali (*data breach*) ai sensi degli artt. 33 e 34 del Regolamento UE 2016/679.

IL CONSIGLIO DI AMMINISTRAZIONE

- VISTO il Decreto legislativo 29 settembre 1999, n. 381, concernente la costituzione dell'Istituto Nazionale di Geofisica e Vulcanologia (INGV);
- VISTO il Decreto Leg.vo 25/11/2016, n. 218, concernente "Semplificazione delle attività degli Enti Pubblici di Ricerca ai sensi dell'art. 13 della Legge 7/08/2015, n. 124";
- VISTO lo Statuto dell'INGV, approvato con Delibera del Consiglio di Amministrazione n. 372/2017 del 9 giugno 2017, come modificato con Delibere del Consiglio di Amministrazione n. 424/2017 del 15 settembre 2017 e n. 501/2017 del 21 dicembre 2017, pubblicato sul Sito WEB istituzionale (Avviso di emanazione pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana - Serie generale - n. 27 del 2 febbraio 2018);
- VISTO il Regolamento di Organizzazione e Funzionamento dell'INGV, emanato con Decreto del Presidente n. 45/2018 del 21/2/2018, pubblicato sul Sito WEB istituzionale;
- VISTO il Regolamento del Personale emanato con Decreto del Presidente n. 118/2018 del 14/5/2018, pubblicato sul Sito WEB istituzionale;
- VISTO il Regolamento di Amministrazione, Contabilità e Finanza, emanato con Decreto del Presidente n. 119/2018 del 14/5/2018, pubblicato sul Sito WEB istituzionale;
- VISTO il Regolamento Unione Europea n. 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016, recepito con Decreto Legislativo n. 101/2018, il quale ha apportato innovazioni e modifiche alla disciplina sulla privacy, contenuta nel Decreto legislativo 30/6/2003, n. 196;
- VISTO il Decreto Direttoriale dell'INGV n. 103 del 09/04/2018, con il quale si procedeva alla nomina del Dott. Lucio Badiali, quale Responsabile della protezione dei dati personali (RDP) per l'Istituto Nazionale di Geofisica e Vulcanologia;
- VISTA la propria Delibera n. 610/2018 del 08/06/2018, con la quale si costituisce l'Ufficio *Data Protection Officer* (DPO) – Nomina dei Responsabili ex Regolamento UE 679/2016;
- VISTO il Decreto Direttoriale dell'INGV n. 312 del 25/10/2018, avente ad oggetto la Costituzione del Gruppo di Lavoro a supporto dell'Ufficio *Data Protection Officer* (DPO);
- VISTI gli artt. 33 e 34 del sopra citato Regolamento sulla Privacy che disciplinano gli obblighi del Titolare in caso di eventi che implichino una violazione dei dati personali trattati (*data breach*);
- TENUTO CONTO che il Titolare del trattamento, ai sensi degli artt. 4 e 24 del Regolamento UE 2016/679, è l'Istituto Nazionale di Geofisica e Vulcanologia, con sede legale in Via di Vigna Murata 605, 00143 Roma, PEC

aoo.roma@pec.ingv.it, nella persona del suo legale rappresentante il presidente *pro-tempore*;

- PRESO ATTO che il Titolare è tenuto a condurre un'analisi dell'evento, al fine di valutarne in modo analitico il potenziale impatto sui diritti e sulle libertà delle persone cui si riferiscono i dati personali violati e in base agli esiti di questo processo di valutazione, il Titolare può essere tenuto a notificare la violazione all'Autorità Garante per la protezione dei dati personali e agli interessati, entro il termine di 72 ore dal momento in cui ne ha conoscenza;
- TENUTO CONTO che la prescrizione del suddetto termine di notifica di 72 ore rende necessaria la formalizzazione di una procedura guidata di analisi, nella quale le figure coinvolte e i rispettivi ruoli siano definiti in modo preciso;
- VISTO il manuale operativo predisposto, il quale risponde a questa esigenza attraverso la definizione di un modello di analisi delle violazioni dei dati personali;
- Su proposta del Presidente,

DELIBERA

la Procedura di gestione delle violazioni dei dati personali (*data breach*), ai sensi degli artt. 33 e 34 del Regolamento UE 2016/679, come previsto dal manuale operativo, allegato alla presente Delibera, della quale costituisce parte integrante e sostanziale.

Letto, approvato e sottoscritto seduta stante.

Roma, 11/10/2019

La segretaria verbalizzante
(Dott.ssa Maria Valeria INTINI)

IL PRESIDENTE
(Prof. Carlo DOGLIONI)

ISTITUTO NAZIONALE DI
GEOFISICA E VULCANOLOGIA

PROCEDURA DI GESTIONE DELLE VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

ai sensi degli artt. 33 e 34 del Regolamento UE n. 2016/679 - Regolamento Generale per la Protezione dei Dati

Titolare del trattamento: Istituto Nazionale di Geofisica e Vulcanologia Via di Vigna Murata, 605 I-00143 Roma Tel. 06518201 PEC aoo.roma@pec.ingv.it	**Responsabile per la Protezione dei Dati:** Lucio Badiali Via di Vigna Murata, 605 I-00143 Roma Tel. 06518601 e-mail dpo@ingv.it

Indice

1. Introduzione

Il Regolamento UE 679/2016, meglio conosciuto come GDPR (General Data Protection Regulation, d'ora in avanti "Regolamento"), è direttamente applicabile negli Stati membri a decorrere dal 25 maggio 2018. Il Regolamento disciplina il trattamento di dati personali, introducendo una serie di obblighi in capo al titolare del trattamento.

In particolare, l'Art. 33 del Regolamento disciplina la gestione degli incidenti che comportino una violazione dei dati personali (c.d. *data breach*). In tali circostanze, il Regolamento prescrive un'analisi dell'incidente, i cui esiti devono essere comunicati all'Autorità Garante entro 72 ore dal momento in cui il Titolare ha avuto notizia dell'evento. Qualora la comunicazione sia effettuata oltre il termine delle 72 ore, deve illustrare i motivi del ritardo. La comunicazione all'autorità può essere omessa qualora l'analisi evidenzi che l'incidente non comporta rischi per i diritti e le libertà delle persone fisiche; al contrario, se l'incidente comporta rischi elevati, la comunicazione deve essere inviata anche agli interessati.

L'esigenza di condurre l'analisi delle violazioni e procedere con le notifiche all'Autorità in tempi rapidi rende necessario codificare e formalizzare in modo preciso la procedura di rilevazione, segnalazione ed analisi delle violazioni, definendo in modo analitico le figure che vi partecipano, i loro ruoli e le loro responsabilità. Il presente documento descrive ed illustra la procedura di gestione ed analisi delle violazioni di dati personali adottata dall'Istituto Nazionale di Geofisica e Vulcanologia.

2. Campo di applicazione

Il presente documento si applica alle violazioni dei dati personali trattati a qualsiasi titolo dall'Istituto Nazionale di Geofisica e Vulcanologia nell'ambito delle proprie attività istituzionali. Ai sensi dell'Art. 4, comma 12 del Regolamento, si intende per «violazione dei dati personali» *la violazione di sicurezza che comporta 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.*

Le violazioni dei dati personali possono essere classificate in base ai seguenti tre principi di sicurezza delle informazioni:

a) **Violazione della riservatezza**: in caso di incidente che comporti la divulgazione o l'accesso non autorizzato o accidentale ai dati personali, portando i medesimi a conoscenza di soggetti estranei al trattamento;
b) **Violazione dell'integrità**: in caso di alterazione non autorizzata, accidentale o comunque non intenzionale dei dati personali;

c) **Violazione della disponibilità**: in caso di accidentale o non autorizzata perdita di accesso o distruzione di dati personali, sia essa temporanea o permanente.

A seconda delle circostanze, una violazione può riguardare un singolo aspetto fra quelli sopra riportati oppure una combinazione di più aspetti.

Sono tenuti all'osservanza delle procedure stabilite nel presente documento, con particolare riguardo alla segnalazione delle violazioni di cui al paragrafo 5, tutti coloro che operino trattamenti di dati personali alle dipendenze dell'Istituto Nazionale di Geofisica e Vulcanologia.

3. Definizioni

Si richiamano qui alcune definizioni utili ai fini della lettura del presente documento. Per l'elenco completo, si rimanda agli Art. 4 e 9 del Regolamento.

- **«dato personale»**: qualsiasi informazione riguardante una persona fisica identificata o identificabile (**«interessato»**); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **«trattamento»**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- **«pseudonimizzazione»**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- **«archivio»**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- **«titolare del trattamento»** (*data controller*): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del

trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

- **«responsabile del trattamento»** (*data processor*): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento; è utile qui precisare che il ruolo di responsabile del trattamento non può essere ricoperto da un dipendente del titolare del trattamento ma solo da un soggetto esterno all'organizzazione del titolare. Il Regolamento stabilisce infatti all'Art. 28 che il rapporto fra titolare e responsabile deve essere regolato *da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*. La figura del responsabile del trattamento, come è stato anche chiarito dal Garante per la protezione dei dati personali, esiste quindi nei soli casi in cui il trattamento avvenga in regime di *outsourcing*.
- **«destinatario»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- **«terzo»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- **«violazione dei dati personali»**: la violazione di sicurezza che comporta 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;
- **«dati relativi alla salute»**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **«Autorità di controllo»**: l'autorità pubblica indipendente istituita da uno Stato membro; in Italia è il Garante per la protezione dei dati personali;
- **«responsabile della protezione dei dati (RPD)»** (*data protection officer*, o DPO): soggetto incaricato almeno dei seguenti compiti: informare e fornire consulenza al titolare del trattamento, al responsabile del trattamento ed ai dipendenti che eseguono attività di trattamento in merito agli obblighi derivanti dal Regolamento; sorvegliare l'osservanza del Regolamento; fornire, ove richiesto, pareri in merito alle valutazioni d'impatto sulla protezione dei dati; cooperare e fungere da punto di contatto con le autorità di controllo.

- **«categorie particolari di dati personali»**: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

4. Figure coinvolte

Nella procedura di gestione delle violazioni dei dati personali sono coinvolte le seguenti figure organizzative, nell'ambito dei rispettivi ruoli e responsabilità:

- **RPD**: Responsabile per la protezione dei dati personali. Svolge i compiti descritti dall'art. 39 del Regolamento e, in particolare, funge da punto di contatto con l'Autorità Garante. Nell'ambito della procedura descritta nel presente documento, il RPD coordina e supervisiona il processo di analisi e valutazione delle violazioni di dati personali e, qualora ne ricorrano i presupposti, ne cura la notifica all'Autorità.

- **RCSI**: Responsabile del Centro Servizi Informativi della sede di Roma.

- **RSIL**: Responsabile dei Servizi Informatici Locali delle sedi diverse dalla sede centrale. Per la sede di Roma coincide con RCSI.

- **ADS**: Amministratore di Sistema, ovvero la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

- **RSO**: Responsabile della Struttura Organizzativa. Nel caso in cui la violazione dei dati personali riguardi un trattamento svolto presso una Sezione, RSO può coincidere con il Responsabile dell'Unità Funzionale (RUF) oppure con il Responsabile della Segreteria Amministrativa (RSA). Nel caso di trattamenti svolti presso l'Amministrazione Centrale, RSO coincide con il Responsabile del Centro Servizi, del Settore o dell'Ufficio che sovrintende al trattamento.

- **DSO**: Dirigente della Struttura Organizzativa. Per le Sezioni coincide con il Direttore di Sezione, mentre in Amministrazione Centrale coincide con il Direttore Centrale di riferimento.

- **RUL**: Rappresentante dell'Ufficio Legale. Coincide con il Responsabile del Settore Affari Legali e Contenzioso presso la Direzione Generale, o con un suo delegato.

5. Modalità di segnalazione delle violazioni

Tutti i soggetti che effettuino trattamenti di dati personali per conto del Titolare del trattamento possono rilevare violazioni dei dati personali. Chiunque rilevi una violazione dei dati personali, anche solo in via potenziale, è tenuto a darne immediata comunicazione con le modalità descritte nel seguito.

5.1. Violazione di dati trattati con strumenti informatici

Nel caso la violazione interessi dati archiviati in formato digitale su basi dati o supporti di memorizzazione informatici, devono essere osservate le seguenti modalità di segnalazione:

1. Chiunque rilevi una violazione, anche solo potenziale, lo comunica a RPD, a RSIL, a RSO ed a DSO. La comunicazione dovrà essere redatta seguendo lo schema fornito in Allegato A e dovrà contenere tutti i dati e le informazioni richieste, ove disponibili.
2. RSIL accerta la reale esistenza della violazione e, in caso sia confermata la violazione stessa, conferma a RPD l'avvenuta violazione.
3. RPD, acquisito un ragionevole grado di certezza del fatto che sia avvenuto un incidente per la sicurezza delle informazioni che abbia compromesso dati personali, riunisce il Nucleo Consultivo per l'Analisi delle violazioni dei dati personali (NCA), costituito da RPD, RCSI, RSO e RUL. Contestualmente, RPD notifica al rappresentante legale del Titolare del Trattamento e per conoscenza al Direttore Generale l'esistenza di una violazione, inserisce una voce per la descrizione della medesima nel "Registro delle violazioni", ed avvia l'analisi della violazione come descritto nel paragrafo 6. Da questo momento decorre il termine di 72 ore previsto dall'Art. 33 del Regolamento.

5.2. Violazione di dati trattati in modalità cartacea

Nel caso la violazione interessi archivi o documenti cartacei devono essere osservate le seguenti modalità per la segnalazione.

1. Chiunque rilevi una violazione, anche solo potenziale, lo comunica a RPD, a RSO ed a DSO. La comunicazione dovrà essere redatta seguendo lo schema fornito in Allegato A e dovrà contenere tutti i dati e le informazioni richieste, ove disponibili.
2. RPD, acquisito un ragionevole grado di certezza del fatto che sia avvenuta un incidente per la sicurezza delle informazioni che abbia compromesso dati personali, riunisce il Nucleo Consultivo per l'Analisi delle violazioni dei dati personali (NCA), costituito da RPD, RCSI, RSO e RUL. Contestualmente, RPD notifica al rappresentante legale del Titolare del Trattamento e per conoscenza al Direttore Generale l'esistenza di una violazione, inserisce una voce per la descrizione della medesima nel "Registro delle violazioni", ed avvia l'analisi della violazione come descritto nel paragrafo 6. Da questo momento decorre il termine di 72 ore previsto dall'Art. 33 del Regolamento.

6. Analisi delle violazioni

Il presente paragrafo descrive i criteri da seguire nel processo di analisi e valutazione del rischio connesso alla violazione di dati personali. Il processo viene avviato in seguito alla conferma dell'esistenza di una violazione, in base a quanto descritto al paragrafo 5, ed è condotto dal Nucleo Consultivo per l'Analisi delle violazioni (nel seguito abbreviato con NCA). Il Nucleo è composto dal RPD, dal RCSI, da RSO e da RUL e svolge il processo di analisi sotto il coordinamento e la supervisione del RPD. Qualora il RPD lo reputi opportuno, il Nucleo può essere integrato con gli ADS dei sistemi informatici sui quali è avvenuta la violazione.

6.1. Valutazione del rischio connesso alla violazione

Per stabilire le modalità di gestione di una violazione e gli eventuali obblighi di notifica RPD, con il supporto del NCA effettua la valutazione del rischio sulla base dei criteri descritti nel seguito.

Il livello di rischio è definito sulla base di due parametri, come di seguito riportati:

a) **gravità**: rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte (es. impedendo il controllo da parte dell'interessato sulla diffusione dei propri dati);
b) **probabilità**: grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).

Ai fini della identificazione dei valori da attribuire ai due parametri per la valutazione del rischio, è possibile considerare i seguenti fattori:

a) tipo di violazione, secondo quanto specificato al paragrafo 5.1;
b) natura, sensibilità e volume dei dati personali;
c) facilità nella identificazione degli interessati;
d) gravità delle conseguenze per gli interessati;
e) particolarità degli interessati (es. minorenni);
f) numero degli interessati.

		Gravità *(Impatto della violazione sui diritti e sulle libertà delle persone coinvolte)*		
		Alta: impatto significativo e irreversibile	**Media:** impatto poco significativo e/o reversibile	**Bassa:** Impatto nullo o trascurabile
Probabilità di accadimento *(Possibilità stimata che si verifichino gli eventi temuti)*	**Alta:** l'evento temuto si è manifestato	Rischio elevato	Rischio elevato	Rischio medio
	Media: l'evento temuto potrebbe manifestarsi	Rischio elevato	Rischio medio	Rischio medio
	Bassa: è improbabile che l'evento temuto si manifesti	Rischio medio	Rischio medio	Rischio basso

Tabella 1 - Matrice decisionale per l'assegnazione del livello di rischio

Livello di rischio	**Notifica all'Autorità**	**Comunicazione agli interessati**
Basso: nessun pregiudizio sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	NO	NO
Medio: possibile pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	NO
Alto: pregiudizio certo sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	SI

Tabella 2 - Azioni da intraprendere in funzione del livello di rischio assegnato

Dunque, sulla base degli elementi di cui sopra:

1. RPD, con il supporto del NCA, stima la gravità e la probabilità della violazione e classifica il rischio, avvalendosi della matrice decisionale riportata in Tabella 1;
2. RPD, previa condivisione della valutazione con il NCA, documenta la decisione presa a seguito della valutazione del rischio nel "Registro delle violazioni", e procede con le azioni riportate in Tabella 2 in funzione del livello di rischio assegnato all'evento:
    a. Nel caso in cui il rischio sia considerato non elevato e non si ritenga necessario procedere con la comunicazione, RPD specifica nel Registro le motivazioni che hanno condotto a tale scelta.
    b. Nel caso in cui l'esito della valutazione del rischio lo richieda, RPD procede alla notifica della violazione all'Autorità.
3. Tutti i dati e gli elementi utilizzati a supporto del procedimento e degli esiti della valutazione del rischio sono documentati da RPD e tale documentazione è conservata.

Qualora lo ritenga opportuno RPD, previa condivisione della decisione con il NCA, può assegnare alla violazione un livello di rischio diverso da quello risultante dalla matrice decisionale in Tabella 1, annotando nel Registro delle Violazione tale decisione e le motivazioni alla sua base.

6.2. Notifica della violazione dei dati personali all'autorità di controllo

L'Art. 33 del Regolamento stabilisce che, qualora una violazione dei dati personali che presenti un rischio di qualsiasi livello superiore al livello "basso" per i diritti e le libertà delle persone coinvolte, è obbligatorio effettuare la notifica all'Autorità.

Per le violazioni così identificate, RPD con il supporto di NCA, redige il documento di notifica della violazione, compilando l'apposito modello presente sul sito dell'Autorità, riprodotto in Allegato B, e la invia all'Autorità di controllo tramite posta elettronica certificata (PEC) all'indirizzo PEC della stessa Autorità (protocollo@pec.gpdp.it).

L'invio avviene entro 72 ore dal momento in cui il Titolare del trattamento è venuto a conoscenza della violazione; tale termine si identifica con il momento in cui RPD, accertata la reale consistenza della violazione segnalata, la notifica al rappresentante legale del Titolare, come descritto nel paragrafo 5. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

In base all'Art. 33 del Regolamento, il documento di notifica deve contenere i seguenti elementi:

- una descrizione della natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo degli interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- una descrizione delle probabili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione;
- qualora la notifica all'autorità di controllo non sia effettuata entro il termine di 72 ore, i motivi del ritardo;
- eventualmente, una dichiarazione sulla mancanza di alcune delle informazioni necessarie e un impegno a fornire, il prima possibile, le informazioni aggiuntive, in una o più fasi successive.

6.3. Comunicazione della violazione dei dati personali agli interessati

Nel caso di accertamento di una violazione dei dati personali che sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, come valutato secondo quanto indicato al paragrafo 6, RPD comunica la violazione anche agli interessati.

In base all'Art. 34 del Regolamento, la comunicazione agli interessarti non è richiesta se è soddisfatta una delle seguenti condizioni:

- 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;
- 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;
- 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.

La comunicazione agli interessati deve essere redatta con un linguaggio semplice e chiaro e deve contenere almeno i seguenti elementi:

- una descrizione della natura della violazione dei dati personali;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- una descrizione delle probabili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione;

Per la comunicazione della violazione agli interessati è possibile identificare uno o più canali di comunicazione, a seconda delle circostanze, quali a titolo di esempio non esaustivo email, SMS, posta ordinaria, banner o notifiche su siti web. La scelta del canale dovrà essere tale da massimizzare la probabilità che tutti gli interessati siano raggiunti dal messaggio.

6.4. Documentazione della violazione

Per ogni violazione di cui sia accertata l'esistenza, RPD compila il "Registro delle violazioni", che riporta:

- numerazione progressiva;
- data di rilevazione;
- struttura/ufficio interessato dalla violazione;
- descrizione della violazione;
- categorie di interessati coinvolti;
- numero approssimativo di interessati in questione
- categorie di dati personali coinvolti;
- volume approssimativo dei dati personali coinvolti;
- cause della violazione;
- conseguenze della violazione;
- misure adottate per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi, con indicazione delle responsabilità e dei tempi per l'attuazione delle misure;
- elementi a supporto della valutazione del rischio: livello di gravità, livello di probabilità, livello di rischio derivante;
- necessità della notifica all'Autorità e data/ora della stessa, ove applicabile;
- necessità della comunicazione all'interessato e data/ora della stessa, ove applicabile.

Ad integrazione di quanto riportato nel registro, RPD raccoglie e conserva tutti i documenti relativi ad ogni violazione, compresi quelli inerenti le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione è resa disponibile all'Autorità di controllo per le verifiche di competenza.

7. Allegati

Allegato A. *Modello per la segnalazione interna delle violazioni*

SEGNALAZIONE DI UNA POSSIBILE VIOLAZIONE DI DATI PERSONALI

1. Breve descrizione della violazione di dati personali

Fornire una breve descrizione dell'evento che ha prodotto o potrebbe produrre una violazione di dati personali.

2. Quando si è verificata la violazione di dati personali?

Fornire tutte le informazioni a disposizione. Ad esempio "il giorno .....", oppure "tra il ..... ed il .....", oppure "in un tempo ancora non determinato". Specificare se è possibile che la violazione sia ancora in corso.

3. Come è avvenuta la violazione dei dati?

Specificare se sia avvenuta a seguito di smarrimento o furto di dispositivi o di supporti portatili, di accesso non autorizzato ad un sistema informatico, di invio per errore di email ad un destinatario sbagliato, di perdita di integrità di dati a causa di guasto hardware o cancellazione accidentale, di furto, smarrimento o distruzione di documenti cartacei, eccetera.

4. Modalità della violazione

Indicare il tipo di violazione fra quelli elencati:

- *lettura (presumibilmente i dati sono stati visionati ma non sono stati copiati)*
- *copia (i dati sono stati copiati ma sono ancora presenti sui sistemi del titolare)*
- *alterazione (i dati sono ancora presenti sui sistemi del titolare ma sono stati alterati)*
- *cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)*
- *furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)*
  altre casistiche che non rientrano nelle precedenti (specificare nel dettaglio).

Indicare il dispositivo (o i dispositivi) oggetto di violazione:

- *sistema di elaborazione centralizzato*
- *personal computer (fisso o portatile)*
- *dispositivo mobile (smartphone, tablet)*
- *sistema di archiviazione centralizzato*

- *supporto di memorizzazione personale (es. Memoria USB, hard disk portatile o da tavolo)*
- *strumento di backup*
- *infrastruttura di rete*
- *documento cartaceo*
- *altro (specificare)*

5. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro funzione ed ubicazione

Qualora la violazione riguardi dati trattati in modalità informatizzata, descrivere i sistemi di elaborazione e/o di archiviazione coinvolti, la loro funzione e la loro ubicazione fisica al momento della violazione.

6. Quante persone sono state colpite dalla violazione di dati personali?

Specificare il numero presunto di interessati i cui dati personali sono coinvolti nella violazione. Se il numero esatto non è noto, fornire una stima approssimativa; qualora non sia possibile nemmeno una stima approssimativa, indicare "un numero ancora sconosciuto di interessati".

7. Che tipo di dati sono coinvolti nella violazione?

Indicare il tipo di dati personali coinvolti nella violazione fra quelli elencati:
- *dati anagrafici*
- *recapiti telefonici e/o di posta elettronica*
- *credenziali di accesso ed identificazione online (username e password)*
- *dati sullo stato di salute*
- *dati sulla situazione reddituale o patrimoniale*
- *dati giudiziari*
- *dati contenenti elementi di appartenenza politica, religiosa o sindacale*
- *altro (specificare)*
- *tipologia di dati ancora sconosciuta*

E' possibile indicare una singola categoria oppure una qualsiasi combinazione di quelle elencate.

8. Livello di gravità della violazione dei dati personali (secondo le valutazioni della persona che effettua la segnalazione)

- *basso/trascurabile*
- *medio*
- *alto*
- *molto alto*

Allegato B. *Modello per la notifica della violazione all'Autorità*

All'Autorità Garante per la protezione dei dati personali
PEC: protocollo@pec.gpdp.it

ISTITUTO NAZIONALE DI GEOFISICA E VULCANOLOGIA
NOTIFICA DI VIOLAZIONE DEI DATI PERSONALI
Ai sensi dell'Art. 33 del Regolamento UE 2016/679

Il sottoscritto _____ in qualità di presidente e legale rappresentante dell'Istituto Nazionale di Geofisica e Vulcanologia (INGV) con sede legale in Roma, Via di Vigna Murata 605, CAP 00143,

NOTIFICA

Ai sensi dell'Art. 33 del Regolamento UE 2016/679 l'avvenuta violazione di dati personali i cui tempi e modalità sono descritti di seguito nel dettaglio.

Data e ora in cui si è verificata la violazione di dati personali: _____

Data e ora in cui il Titolare del Trattamento è venuto a conoscenza della violazione:

_____

_____

_____

Attenzione: *ove la notifica* ***non sia effettuata nelle 72 ore successive*** *al momento in cui il Titolare è venuto a conoscenza della violazione, è necessario precisare i motivi che non hanno consentito la notifica entro il termine prescritto dal Regolamento UE 2016/679.*

Breve descrizione della violazione dei dati personali:

_____

_____

Modalità della violazione dei dati personali (specificare ad esempio se sia avvenuta in seguito a smarrimento di dispositivi o di supporti portatili):

_____

_____

Modalità di esposizione al rischio (indicare tutte le voci pertinenti):

- Lettura (i dati sono stati visionati ma presumibilmente non sono stati copiati);
- Copia (i dati sono stati copiati ma sono ancora presenti negli archivi del Titolare);

- Alterazione (i dati sono presenti negli archivi del Titolare ma sono stati alterati);
- Cancellazione (i dati non sono più presenti negli archivi del Titolare, e non li possiede neppure l'autore della violazione);
- Furto (i dati non sono più presenti negli archivi del Titolare, ma sono in possesso dell'autore della violazione);
- Altro (specificare).

Dispositivi e/o archivi oggetto della violazione (indicare tutte le voci pertinenti:

- Computer
- Dispositivo mobile
- Documento cartaceo
- File o parte di un file
- Strumento di backup
- Rete informatica
- Altro (specificare)

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, ovvero degli archivi cartacei coinvolti, con indicazione della loro ubicazione:

Categorie di dati personali interessati dalla violazione:

Numero (anche approssimativo) di persone i cui dati sono stati violati:

Livello di gravità della violazione dei dati personali risultante dalle analisi condotte:

Misure tecniche ed organizzative applicate ai dati colpiti dalla violazione:

Data ed ora dell'eventuale comunicazione della violazione alle persone interessate (qualora non sia stata effettuata, specificare i motivi per cui non è stata ritenuta necessaria):

Contenuto della comunicazione della violazione alle persone interessate (solo nel caso in cui sia stata effettuata):

Canale utilizzato per la comunicazione della violazione alle persone interessate:

Eventuali misure tecniche e/o organizzative che sono state assunte per contenere la violazione e prevenire simili violazioni future:

Nominativo del DPO e dati di contatto:

Si dichiara che tutta la documentazione inerente la violazione dei dati personali, incluse le circostanze in cui si è verificata, le sue conseguenze ed i provvedimenti adottati per porvi rimedio sono disponibili presso il Titolare del Trattamento, e si resta altresì a disposizione per fornire ogni eventuale informazione richiesta.

Il Presidente

***Allegato C**. Modello per la comunicazione della violazione agli interessati*

Gentile _____,

La informiamo che in data _____ siamo venuti a conoscenza di un evento che potrebbe aver coinvolto i Suoi dati personali.

Presumiamo che in data _____, alle ore _____, persone non autorizzate abbiano avuto accesso a dati personali che la riguardano. In dettaglio, i dati personali violati riguardano le seguenti categorie di informazioni:

_____
_____
_____

Sulla base della nostra analisi, le possibili conseguenze dell'evento sono:

_____
_____
_____
_____

In risposta all'evento, abbiamo adottato le seguenti misure di sicurezza volte a mitigare l'impatto della violazione:

_____
_____
_____
_____

Per sua maggiore sicurezza, La invitiamo a intraprendere le seguenti azioni:

_____
_____
_____
_____

Per qualsiasi informazione o chiarimento, può contattare _____ ai seguenti recapiti: _____.

Allegato D. *Modello di scheda del Registro delle Violazioni*

Numero progressivo	
Data e ora di rilevazione	
Strutture/uffici coinvolti	
Descrizione della violazione	
Categorie di interessati e numero approssimativo di interessati per categoria	
Categorie di registrazioni di dati personali e numero approssimativo di registrazioni coinvolte per categoria	
Cause della violazione	
Conseguenze della violazione	
Misure di sicurezza previste e data della loro attuazione	
Gravità stimata dei potenziali effetti pregiudizievoli della violazione	
Probabilità stimata di accadimento dei potenziali effetti pregiudizievoli della violazione	
Necessità di notifica all'Autorità	
Data e ora di notifica all'Autorità, qualora necessaria	
Necessità di comunicazione agli interessati	
Data e ora di comunicazione agli interessati, se necessaria	