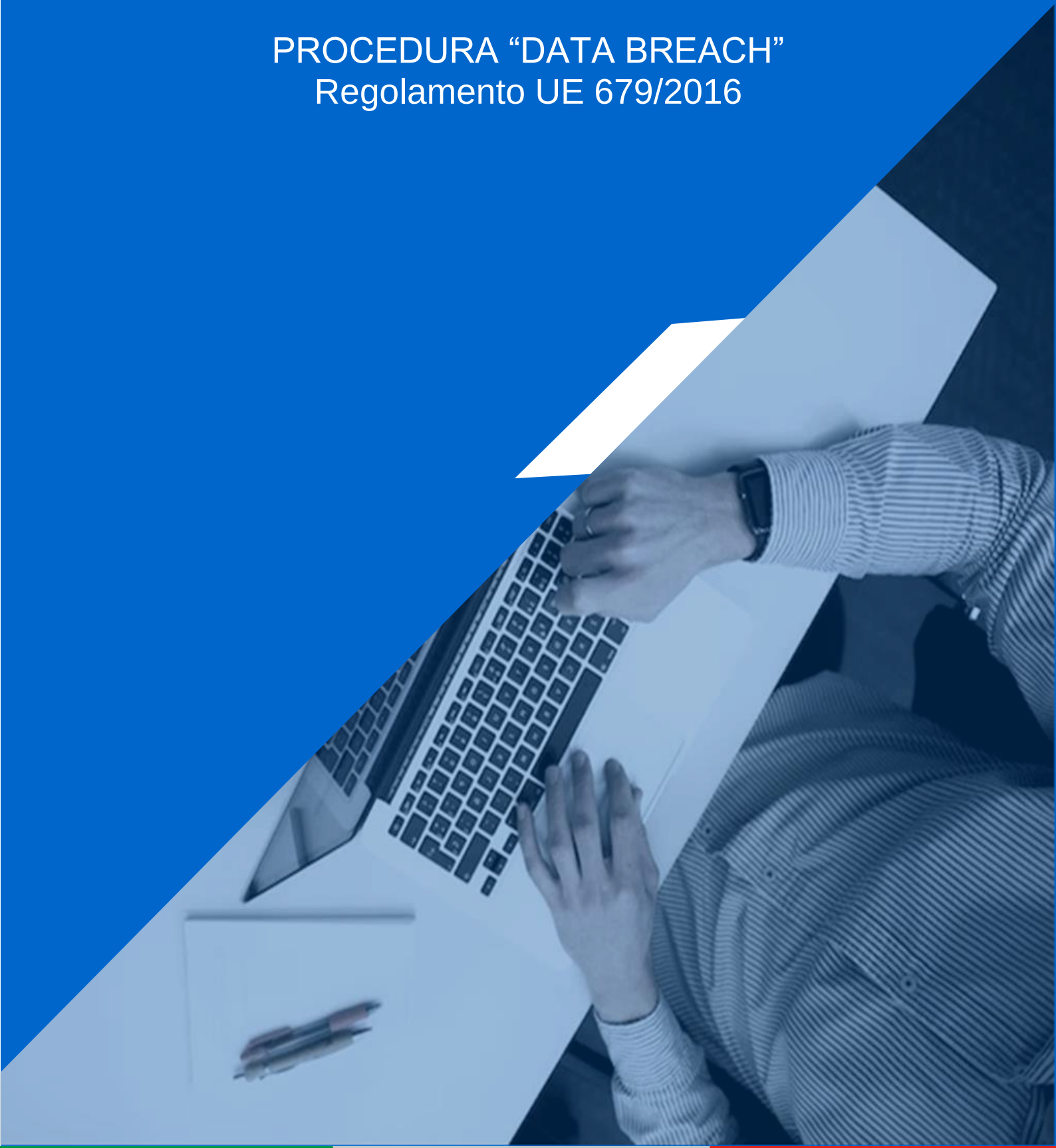
FORMEZ

AL SERVIZIO DELLA PA

PROCEDURA “DATA BREACH”
Regolamento UE 679/2016



SOMMARIO

Titolo	PROCEDURA DATA BREACH - Regolamento UE 679/2016
Tipologia di documento	Procedura
Data di entrata in vigore	01/10/2023
Responsabile	Affari legali, compliance e controllo qualità progetti – Responsabile DPO

Versioni e Responsabilità

Versione	Data di emissione	Dettaglio modifiche apportate	Responsabile
1	20/07/2023	Prima emissione	Affari legali, compliance e controllo qualità progetti – Responsabile DPO

Procedure di Formez PA correlate

- Procedura Formez PA “DPIA - Data Protection Impact Assessment, Regolamento UE 679/2016”, 25/07/2018;

ALLEGATI

- N/A

INDICE

DEFINIZIONI E ABBREVIAZIONI

Termine	Acronimo	Definizione
ARCHIVIO	**N/A**	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
AUTORITA' DI CONTROLLO/ AUTORITA'	**N/A**	L'autorità pubblica indipendente istituita da uno Stato membro; in Italia è il Garante per la protezione dei dati personali.
CONSENSO DELL'INTERESSATO	**N/A**	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
DATI BIOMETRICI	**N/A**	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
DATI GENERICI	**N/A**	I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
DATI RELATIVI ALLA SALUTE	**N/A**	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.
DATO PERSONALE	**N/A**	Qualsiasi informazione riguardante una persona fisica identificata o identificabile
DESTINATARIO	**N/A**	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

Termine	Acronimo	Definizione
		materia di protezione dei dati secondo le finalità del trattamento
GRUPPO IMPRENDITORIALE	**N/A**	Un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate.
IMPRESA	**N/A**	La persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica
LIMITAZIONE DI TRATTAMENTO	**N/A**	Il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro
NORME VINCOLANTI D'IMPRESA	**N/A**	Le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune.
PROFILAZIONE	**N/A**	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica
PSEUDONIMIZZAZIONE	**N/A**	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
RAPPRESENTANTE	**N/A**	La persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento.

Termine	Acronimo	Definizione
RESPONSABILE AREA INNOVAZIONE DIGITALE	**RAID**	È il dirigente all'interno della PA che garantisce operativamente la trasformazione digitale dell'amministrazione, coordinando lo sviluppo dei servizi pubblici digitali e l'adozione di nuovi modelli di relazione con i cittadini, trasparenti e aperti. Nell'area organizzativa di Formez PA, tale ruolo ricade nella figura del responsabile "Information And Communication Technology"
RESPONSABILE DEL TRATTAMENTO	**N/A**	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Nell'area organizzativa di Formez PA, tale ruolo ricade nella figura del Responsabile DPO dell'area "Affari legali, compliance e controllo qualità progetti"
RESPONSABILE DELLA TUTELA DEI DATI PERSONALI E DELLA TUTELA DEI DATI AZIENDALI	**RTDP**	La persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo per suo conto del trattamento dei dati. Nella struttura organizzativa di Formez PA, tale ruolo ricade nella figura del Responsabile DPO dell'area "Affari legali, compliance e controllo qualità progetti"
RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI	**RPD**	La persona fisica o giuridica che ha il compito di informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché ai loro dipendenti, sui loro obblighi ai sensi della legge sulla protezione dei dati; verificare il rispetto da parte dell'organizzazione di tutta la legislazione in materia di protezione dei dati, anche per quanto riguarda gli audit, le attività di sensibilizzazione e la formazione del personale addetto al trattamento dei dati; fungere da punto di contatto per le richieste degli interessati relative al trattamento dei loro dati personali e all'esercizio dei loro diritti; collaborare con le autorità di protezione dei dati e fungere da punto di contatto per le stesse su questioni relative al trattamento. Nella struttura organizzativa di Formez PA, tale ruolo ricade nella figura del Responsabile DPO dell'area "Affari legali, compliance e controllo qualità progetti"
STABILIMENTO PRINCIPALE	**N/A**	a) Per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in

Termine	Acronimo	Definizione
		un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento
TERZO	**N/A**	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
TITOLARE DEL TRATTAMENTO	**N/A**	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. Nella struttura organizzativa di Formez PA, tale ruolo ricade nella figura del Presidente.
TRATTAMENTO	**N/A**	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

Termine	Acronimo	Definizione
		raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione
VIOLAZIONE DEI DATI PERSONALI	**N/A**	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.

Tabella 1: Elenco definizioni per termine / acronimo

1. INTRODUZIONE

1.1. Obiettivi del documento

Nel presente documento si definiscono attività, ruoli, responsabilità ed eventuale strumentazione informatica utilizzati per illustrare la procedura “Data Breach”.

Lo scopo della procedura è quello di definire le modalità e le responsabilità per effettuare:

- La notifica di una violazione dei dati personali all'autorità di controllo;
- La comunicazione di una violazione dei dati personali all'interessato; garantendo altresì:
  - L’identificazione della violazione;
  - L’analisi delle cause della violazione;
- La definizione delle misure da adottare per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi;
- La registrazione delle informazioni relative alla violazione, delle misure identificate e dell'efficacia delle stesse.

1.2 Campo di applicazione

Il documento descrive la procedura e le attività operative svolte da Formez PA con particolare riferimento alla gestione di tutti gli archivi/ documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati (clienti, fornitori, altri soggetti terzi), anche con il supporto di fornitori esterni.

2. CONTESTO NORMATIVO E PROCEDURALE DI RIFERIMENTO

Il documento descrive le attività operative per la procedura in oggetto, in conformità con quanto definito da:

- **Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio** del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- **Linee guida sulla notifica delle violazioni di dati personali** ai sensi del Regolamento 679/2016 (WP250), adottate dal Gruppo di lavoro Articolo 29 ("WP29"), in via definitiva, il 6 febbraio 2018; (AGGIORNAMENTO: Linee guida 9/2022 in materia di notifica delle violazioni di dati personali (data breach))
- **Linee guida concernenti la valutazione di impatto sulla protezione dei dati** nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679 (WP248), adottate dal WP29, in via definitiva, il 4 ottobre 2017;
- **Linee guida EDPB 01/2021** sugli esempi riguardanti la notifica di violazione dei dati
- **Linee guida sui responsabili della protezione dei dati (WP243)**, adottate dal WP29, in via definitiva, il 5 aprile 2017;
- **Dichiarazione relativa al ruolo di un approccio basato sul rischio** nel quadro normativo in materia di protezione dati (WP218), adottata dal WP29 il 30 maggio 2014;
- **Raccomandazioni per una metodologia della valutazione della gravità delle violazioni di dati personali**, adottate dalla European Union Agency for Network and Information Security (ENISA) il 20 dicembre 2013;
- **Linee guida 07/2020** sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR, Versione 2.0, adottate il 7 luglio 2021;
- **Provvedimento del 27 maggio 2021** - Procedura telematica per la notifica di violazioni di dati personali (data breach);
- **Agenda digitale europea; à Ultimo aggiornamento 2019 - Informativa Sul Trattamento Dei Dati Personali**
- **Decreto Legislativo 30 giugno 2003 n. 196**, recante il "Codice in materia di protezione dei dati personali" e provvedimenti adottati dall'Autorità Garante per la protezione dei dati personali;
- **Decreto Legislativo 25 gennaio 2010, n. 6** – "Riorganizzazione del Centro di formazione studi (FORMEZ), a norma dell'articolo 24 della legge 18 giugno 2009, n. 69. (10G0025)"
- **Linee guida dell'Agenzia per l'Italia digitale – AgID;**
- **Il Codice dell'Amministrazione Digitale (CAD-DLgs 82/2005);**
- **Best practices di settore** sviluppatesi alla luce del Codice e della giurisprudenza del Garante;
- **Nuovo statuto di Formez PA** (adottato dall'Assemblea Straordinaria degli Associati di Formez PA con la deliberazione n. 60 del 20 giugno 2023 e approvato con decreto del Ministro per la Pubblica Amministrazione dell'11 luglio 2023);
- **Regolamento interno di organizzazione, contabilità e amministrazione di Formez PA** adottato dall'Assemblea Ordinaria degli Associati con la deliberazione n. 61 del 20 giugno 2023;

- **Procedura "DPIA - Data Protection Impact Assessment, Regolamento UE 679/2016**", 25/07/2018 di Formez PA

3. ATTIVITÀ OGGETTO DEL DOCUMENTO

La seguente sezione ha come obiettivo quello di illustrare le diverse fasi di cui si compone la procedura "Data Breach".

3.1 Individuazione della violazione

Per violazione dei dati personali si intente una 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 (un esempio possono essere i dati di natura anagrafica, numeri di carte personali, codici identificativi, dati sanitari, dati biometrici, dati relativi a conti correnti, ecc.).

Queste violazioni possono essere classificate in base ai seguenti principi di sicurezza delle informazioni:

1. **Violazione della riservatezza:** in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
2. **Violazione dell'integrità:** in caso di alterazione non autorizzata o accidentale dei dati personali;
3. **Violazione della disponibilità**: in caso di accidentale o non autorizzata perdita di accesso o distruzione di dati personali.

A seconda delle circostanze, una violazione può riguardare tutti gli aspetti sopra indicati o una combinazione di essi.

Tutti possono rilevare violazioni dei dati personali (di seguito "violazioni").

3.2. Segnalazione della violazione

3.3.1 Violazione di dati digitalizzati

Qualora la violazione dovesse interessare dati archiviati in formato digitale su basi dati o supporti di memorizzazione - messi a disposizione dal sistema informativo di Formez PA – le modalità di segnalazione da osservare, vengono elencate di seguito:

1. Colui che rileva la violazione lo deve comunicare al **RAID** e per conoscenza al **RPD** fornendo i dati in suo possesso (presenti nel modello semplificato in Allegato 5).
2. Una volta segnalato ciò:
    a) Il **RAID** accerta la reale esistenza della violazione e, in caso sia confermata la violazione stessa, conferma a RPD l'avvenuta violazione.
    b) Il **RPD**, acquisito un ragionevole grado di certezza del fatto, inserisce una voce per la descrizione del data Breach nel "*Registro delle violazioni*".

Nell'allegato 4 "*Scenari di Data Breach*", inoltre, viene riportato un *elenco* esemplificativo di eventi da cui possono derivare violazioni dei dati personali, con indicazione della necessità di notifica e di comunicazione.

3.2.2 Violazione di dati su supporti fisici o informatizzati personali

Qualora la violazione dovesse interessare archivi o documenti cartacei o informazioni digitalizzate - contenute su supporti fisici di memorizzazione non gestiti dal sistema informativo di Formez PA - le modalità di segnalazione da seguire vengono riportate di seguito:

1. Colui che rileva la violazione lo deve comunicare al **RPD,** fornendo i dati in suo possesso presenti nel modello semplificato in Allegato 5.
2. L**'RPD**, acquisito un **ragionevole grado di certezza** dell'accaduto, inserisce una apposita voce per la descrizione del data Breach nel "Registro delle violazioni".

3.3 Valutazione del rischio connesso alla violazione

Per identificare le modalità di gestione di una violazione e gli eventuali obblighi di notifica e/o di comunicazione, l'**RPD** (con il supporto di RAID nel caso di dati digitalizzati gestiti dal sistema informativo Formez PA) effettua la valutazione del rischio, come di seguito indicato.
Il livello di rischio è definito sulla base di due parametri:

- **Gravità**: si intende la rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sia sui diritti che sulle libertà delle persone coinvolte (es. impedendo il controllo da parte dell'interessato sulla diffusione dei propri dati);
- **Probabilità**: si intende il 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:

- Il tipo di violazione;
- La natura, sensibilità e volume dei dati personali;
- La facilità nella identificazione degli interessati;
- La gravità delle conseguenze per gli interessati;
- La particolarità degli interessati (es. bambini);
- La particolarità dei responsabili del trattamento (es. personale sanitario);
- Il numero degli interessati.

Gravità	Impatto della violazione sui diritti e le libertà delle persone coinvolte: ▪ **1 - Basso**: nessun impatto ▪ **2 - Medio**: impatto poco significativo, reversibile ▪ **3 - Alto**: impatto significativo, irreversibile
Probabilità	Possibilità che si verifichino uno o più eventi temuti: ▪ **1 - Basso**: l'evento temuto non si manifesta ▪ **2 - Medio**: l'evento temuto potrebbe manifestarsi ▪ **3 - Alto**: l'evento temuto si è manifestato

Sulla base della valutazione circa la gravità della violazione e la relativa probabilità che la stessa si verifiche (Gravità x Impatto), possono aprirsi diversi scenari che vengono elencati in tabella:

	Descrizione	Notifica all'Autorità	Comunicazione agli interessati
Rischio	1-3 - Basso: nessun pregiudizio sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	NO	NO
	4-6 - Medio: possibile pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	NO
	9 - Alto: pregiudizio certo sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	SI

Sulla base degli elementi di cui sopra:

1. **RPD** stima la gravità e la probabilità della violazione e classifica il rischio;
2. **RPD**, previa condivisione della valutazione con RTDP, documenta la decisione presa a seguito della valutazione del rischio nel "Registro delle violazioni", nei seguenti modi:
    a) ***Rischio non elevato****: l'*RPD specifica la giustificazione per tale scelta.
    b) **Rischio elevato**: l'RPD procede alla notifica della violazione (§ 3.4)
3. Gli elementi a supporto del procedimento e degli esiti della valutazione del rischio sono documentati da RPD e tale documentazione è conservata come da § 3.8.
4. Al fine di attestare il momento in cui si è venuti a conoscenza della violazione, l'RPD la segnala tramite e-mail - al Titolare del trattamento Formez PA, inviandogli adeguate informazioni circa la natura e gli esiti della valutazione del rischio di cui sopra.

Per maggiori informazioni in merito all'argomento, si segnala la procedura "DPIA - Regolamento UE 679/2016".

3.4 Notifica della violazione dei dati personali all'autorità di controllo

La normativa vigente prevede che, non appena si venga a conoscenza di una violazione dei dati personali per i diritti e le libertà delle persone coinvolte[1], è obbligatorio effettuare la notifica all'Autorità.

- Per le violazioni così identificate, l'RPD con il supporto del RAID, redige il documento di notifica della violazione, compilando l'apposito modello presente sul sito dell'Autorità, riprodotto in Allegato 2 "*Notifica*", e la invia all'Autorità di controllo tramite posta elettronica certificata (PEC) all'indirizzo (dcrt@pec.gpdp.it).
- L'invio avviene entro 72 ore dal momento in cui il titolare del trattamento ne è venuto a conoscenza (tale momento si identifica con l'invio della e-mail al Presidente), 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.

È opportuno segnalare, inoltre, che il documento di notifica deve contenere almeno i seguenti elementi:

1. **La natura della violazione dei dati personali**, compresi, ove possibile:
    a. le categorie e il numero approssimativo di interessati;
    b. le categorie e il numero approssimativo di registrazioni dei dati personali in questione.
2. **Il nome e i dati di contatto del responsabile della protezione dei dati** o di altro punto di contatto presso cui ottenere più informazioni;
3. **Le probabili conseguenze** della violazione dei dati personali;
4. **Le misure adottate** o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione;
5. **I motivi del ritardo**, qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore;
6. **Una dichiarazione sulla mancanza di alcune delle informazioni necessarie** e un **impegno a fornire le informazioni aggiuntive**, in una o più fasi successive.

3.5 Comunicazione della violazione dei dati personali a interessato/i

Nel caso di un accertamento di una violazione dei dati personali, che presenti un rischio elevato per i diritti e le libertà delle persone fisiche, l'RPD comunica la violazione all'interessato (con le modalità illustrate al paragrafo 3.2).

La comunicazione **non** sarà necessaria, qualora vengano soddisfatte almeno una delle seguenti condizioni:

- Il titolare del trattamento abbia messo in atto le misure tecniche/organizzative di protezione e che tali misure siano state anche applicate anche ai dati personali, oggetto della violazione;

[1] che presenti un rischio di qualsiasi livello superiore a quello "basso

- Il titolare del trattamento abbia successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- Se la suddetta comunicazione richiedesse sforzi sproporzionati: è possibile procede con l'adozione di una comunicazione pubblica o a una misura simile, tramite la quale gli interessati siano informati con analoga efficacia.

La comunicazione deve contenere almeno i seguenti elementi:

- **La natura della violazione dei dati personali**, descritta con linguaggio semplice e chiaro;
- **Il nome e i dati di contatto del responsabile** della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- **Le probabili conseguenze** della violazione dei dati personali;
- **Le misure adottate o di cui si propone l'adozione** da parte del titolare del trattamento per porre rimedio alla violazione.

Per la comunicazione, inoltre, è possibile identificare uno o più canali di comunicazione, scegliendo quello che massimizzi la probabilità che tutti gli interessati siano raggiunti dal messaggio:

- E-mail;
- SMS;
- Posta;
- Comunicati pubblicitari;
- Banner;
- Notifiche su siti web.

3.6 Documentazione della violazione

Per ogni violazione di cui sia accertata l'esistenza, RPD compila il "Registro delle violazioni", riportando i seguenti dati:

- Numerazione progressiva;
- Data di rilevazione;
- Area/ processo interessato dalla violazione;
- Descrizione della violazione;
- Categorie di interessati in questione;
- Numero approssimativo di interessati in questione;
- Categorie di registrazioni dei dati personali in questione;
- Numero approssimativo di registrazioni dei dati personali in questione;
- Cause della violazione;
- Conseguenze della violazione;
- Misure 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 alla Autorità e data/ ora della stessa, ove applicabile;

- Necessità della comunicazione all'interessato e data/ ora della stessa, ove applicabile;
- Verifica dell'attuazione delle misure;
- Verifica dell'efficacia delle misure.

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

3.7 Controlli

Qualora siano identificati più titolari del trattamento (es. caso di responsabili esterni del trattamento o di titolari autonomi); i ruoli e le responsabilità tra le parti sono stati definiti preliminarmente con la "*Nomina di responsabile esterno del trattamento*": ovvero, con la "*clausola privacy*" sottoscritte dal soggetto esterno, per la gestione degli obblighi di notifica e di comunicazione in caso di violazione dei dati personali.

In questi casi, il titolare del trattamento con il supporto di RPD concorda con i responsabili esterni del trattamento (o titolari autonomi) le modalità per la gestione degli obblighi di notifica e di comunicazione in caso di violazione dei dati personali, al fine di garantire il rispetto dei termini di notifica e di comunicazione, di cui il titolare del trattamento resta legalmente responsabile.

3.8 Archiviazione

Gli allegati "Notifica" e "Comunicazione" e tutti i documenti relativi alle notifiche ed alle comunicazioni sono archiviati da RPD sul sistema di archiviazione documentale di Formez PA. Il "Registro delle violazioni" e il documento "Scenari di Data Breach" sono archiviati da RPD sul sistema di archiviazione documentale di Formez PA.

4. RESPONSABILITÀ

Attività	Responsabile	Altri attori coinvolti (eventuali)	Tempistiche
3.1 INDIVIDUAZIONE DELLA VIOLAZIONE			
3.1.1 Segnalazione violazione dati personali con annessa comunicazione al RAID e RPD	SOGGETTO PERSONA FISICA	N/A	3 giorni
3.2 SEGNALAZIONE DELLA VIOLAZIONE			
3.2.1 Accertamento ed eventuale conferma dell'esistenza della violazione (solo in caso di violazione di dati digitalizzati)	RAID	N/A	2 giorni
3.2.2 Inserimento, in caso di ragionevole grado di certezza del fatto che è avvenuto un data breach, della voce per la descrizione dell'incidente nel "Registro delle violazioni"	RPD	N/A	30 giorni
3.3 VALUTAZIONE DEL RISCHIO CONNESSO ALLA VIOLAZIONE			
3.3.1 Valutazione rischio della violazione dei dati personali (stima di gravità, probabilità della violazione e classificazione del rischio)	RPD	RAID (nel caso di dati digitalizzati gestiti dal sistema informativo Formez PA)	30 giorni
3.4 NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ DI CONTROLLO			
3.4.1 Redazione del documento di notifica della violazione	RPD	RAID (nel caso di dati digitalizzati gestiti dal sistema informativo Formez PA)	15 giorni
3.4.2 Invio del documento, entro le 72 ore, dal momento in cui	RPD	AUTORITA' DI CONTROLLO	4 giorni

Attività	Responsabile	Altri attori coinvolti (eventuali)	Tempistiche
il titolare del trattamento ne è venuto a conoscenza			
3.5 COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI A INTERESSATO/I			
3.5.1 Comunicazione della violazione dei dati personali a interessato/i in caso di accertamento della violazione dei dati personali con rischio elevato per i diritti e le libertà delle persone e negli altri casi previsti.	RPD	INTERESSATO/I	3 giorni
GIORNI TOTALI PER IL COMPLETAMENTO DELLA SEZIONE			**87 giorni**

Attività	Responsabile	Altri attori coinvolti (eventuali)	Tempistiche
3.6 DOCUMENTAZIONE DELLA VIOLAZIONE			
3.6.1 Raccolta di tutti i documenti relativi ad ogni violazione, conseguenze e provvedimenti adottati per porvi rimedio.	RPD	N/A	Entro 30 giorni
3.6.2 Invio documentazione all'autorità di controllo per le verifiche di competenza.	RPD	AUTORITA' DI CONTROLLO	
GIORNI TOTALI PER IL COMPLETAMENTO DELLA SEZIONE			**30 giorni**

3.7 CONTROLLI			
3.7.1 Concorda le modalità per la gestione degli obblighi di notifica e di comunicazione in caso di violazione dei dati personali.	TITOLARE DEL TRATTAMENTO/ RPD	RESPONSABILI ESTERNI	30 giorni
GIORNI TOTALI PER IL COMPLETAMENTO DELLA SEZIONE			**30 giorni**

Attività	Responsabile	Altri attori coinvolti (eventuali)	Tempistiche

Attività	Responsabile	Altri attori coinvolti (eventuali)	Tempistiche
3.8 ARCHIVIAZIONI			
3.8.1 Archiviazione del Registro delle violazioni e del documento “Scenari Data Breach” sul sistema di archiviazione documentale di Formez PA.	RPD	N/A	Entro 90 giorni[2]
GIORNI TOTALI PER IL COMPLETAMENTO DELLA SEZIONE			**90 giorni**

Tabella 2: Rappresentazione delle responsabilità e di eventuali altri attori coinvolti per attività

[2] Attività esclusa dal conteggio dei giorni totali per il completamento della procedura