Allegato A - **Manuale per la gestione di una violazione di dati personali (Data Breach)**

Approvato con deliberazione della Giunta Comunale n.141 del 19/08/2025

Sommario

Finalità

Il presente documento va ad integrare il Modello Organizzativo per l'attuazione del Regolamento Europeo N.679 del 2016 e del Codice Privacy D.Lgs. 196 del 2003 relativamente alla protezione dei dati personali delle persone fisiche, adottato dal Comune di Porto Sant'Elpidio approvato con deliberazione Giunta Comunale n.199 del 04/05/2021.

Esso indica le modalità di gestione di una violazione dei dati personali (data breach), di cui il Comune di Porto Sant'Elpidio è Titolare, con l'intento di limitare i rischi per i diritti e le libertà dei singoli, considerando che l'efficacia dell'intervento dipende dalla tempestività e dall'adeguatezza delle misure adottate, nel rispetto delle disposizioni normative in materia.

Nella redazione del presente Manuale si è tenuto conto, in particolare, delle indicazioni e delle disposizioni:

- del Regolamento Europeo UE 2016/679 (d'ora innanzi "GDPR");
- del Dlgs. 30 giugno 2003 n.196 "Codice in materia di protezione dei dati personali" e successive modifiche ed integrazioni;
- delle Linee guida sulla notifica delle violazioni di dati personali ai sensi del Regolamento UE 2016/679 WP250 rev.01 del Gruppo di lavoro Art.29 nella versione emendata e adottata il 6 febbraio 2018;
- del Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni di dati personali.

Ambito di Applicazione - Destinatari

L'art.32 ("*Sicurezza del trattamento*") del GDPR prevede che, nell'attuare misure tecniche ed organizzative per garantire un livello di sicurezza adeguato, occorre, tra l'altro, prendere in considerazione " *la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento"* e " *la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico* "

Il presente Manuale costituisce una guida per tutti i soggetti indicati nel Modello Organizzativo del Comune ovvero dirigenti, dipendenti, responsabili esterni del trattamento ed in genere per tutti i soggetti terzi autorizzati ad accedere ad archivi e a documenti cartacei, alla rete comunale e ai sistemi informatici del Comune di Porto Sant'Elpidio.

Le prescrizioni del presente Manuale integrano le specifiche istruzioni impartite ai responsabili e agli incaricati del trattamento in materia di privacy.

Il mancato rispetto delle istruzioni di cui al presente Manuale costituisce, per dirigenti e dipendenti, violazione del Codice di comportamento e determina, nel rispetto dei principi di gradualità e proporzionalità, l'applicazione delle sanzioni disciplinari previste dalle disposizioni di legge e dal Contratto Collettivo Nazionale di Lavoro vigente, fatto salvo comunque il diritto del Comune al risarcimento dei danni eventualmente patiti a causa della condotta del lavoratore.

Il mancato rispetto delle regole e dei divieti del presente Manuale costituisce, per i responsabili esterni del trattamento, violazione degli obblighi contrattuali. Al momento della nomina, il responsabile esterno del trattamento dichiara di avere preso visione del presente Manuale e degli adempimenti in esso previsti.

Tutti i Destinatari sono tenuti a conoscere ed applicare il presente Manuale, al quale verrà data la massima pubblicità, mediante la pubblicazione sul sito istituzionale del Comune: https://comune.portosantelpidio.fm.it**.**

Definizioni

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 riferimento ad un identificativo come il nome, un numero di identificazione, un identificativo on line, dati relativi all'ubicazione o uno o più elementi della sua identità fisica, genetica, psichica, economica, culturale o sociale.

Il concetto di dato personale ricomprende qualunque contenuto che fornisca informazioni su una persona fisica. Non è unicamente un nome, un cognome, una data di nascita, un numero di telefono, l'indirizzo di posta elettronica, un dato testuale, ma, a titolo puramente esemplificativo, anche un'immagine, la registrazione di una voce, una videoripresa, un numero di targa.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a 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;

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;

Titolare del trattamento ("Titolare"): 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;

Responsabile del trattamento ("Responsabile"): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Violazione Dei Dati Personali (Data Breach) : si definisce "Violazione della sicurezza dei dati personali" la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato a dati personali trasmessi, conservati o comunque trattati, sia per motivi accidentali che illeciti.

In dettaglio, possiamo specificare che si ha:

- **"*distruzione*"** dei dati quando i dati non esistono più o non esistono più in una forma che sia utile al titolare del trattamento;
- ***"danno"*** quando i dati personali sono stati modificati, corrotti o non sono più completi;
- ***" perdita"*** quando il titolare ha perso il controllo o il possesso dei dati o non può più accedervi
- ***"trattamento non autorizzato o illecito"*** quando viene effettuata una divulgazione non autorizzata di dati personali, l'accesso da parte di destinatari non autorizzati a ricevere i dati o, in genere, qualsiasi forma di trattamento in violazione delle disposizioni normative o dell'Ente in materia di privacy.

Inoltre, le violazioni sono sintetizzabili come

- ***Violazione di confidenzialità*** in caso di divulgazione o accesso non autorizzato o accidentale ai dati (ad esempio nel caso di dati personali che, per errore o a seguito di un attacco informatico, vengono pubblicati o che vengono inviati ad un indirizzo sbagliato);
- ***Violazione dell'integrità*** in caso di alterazione non autorizzata o accidentale dei dati;
- ***Violazione della disponibilità*** in caso di accidentale o non autorizzata perdita di accesso o distruzione dei dati personali (ad esempio nel caso di dati cancellati accidentalmente o da

persona non autorizzata; nel caso di interruzione di corrente significativa che comporta la perdita temporanea della disponibilità di dati personali)

Una violazione può riguardare contemporaneamente la confidenzialità, l'integrità e la disponibilità dei dati personali.

Comitato per la gestione delle segnalazioni

È istituito presso l'Ente il "Comitato per la gestione delle violazioni dei dati personali" ("Comitato"), al fine di garantire una adeguata, tempestiva ed uniforme gestione delle violazioni dei dati personali.

Esso rappresenta il punto di riferimento unico a cui il personale dell'Ente deve rivolgersi per segnalare una potenziale violazione dei dati personali oppure un comportamento sospetto.

Esso ha il compito di

- gestire tutte le attività inerenti l'analisi e la gestione delle violazioni, ivi comprese quelle relative alla sua notifica e documentazione;
- garantire la disponibilità delle liste di contatti (es.: personale dipendente, collaboratori, fornitori), necessarie per la gestione di un incidente di sicurezza;
- garantire che il processo di gestione delle violazioni sia sempre adeguato alle esigenze dell'Ente, provvedendo che sia sempre aggiornato.

Il Comitato è formato dalle persone fisiche che rivestono pro tempore i seguenti ruoli organizzativi :

Ruolo	**Compiti nel Comitato**
Titolare del trattamento - Rappresentante legale dell'Ente: Sindaco	Responsabilità generale della gestione delle violazioni, incluse le comunicazioni con l'Autorità di controllo
Responsabile per la protezione dei dati - DPO	Valutazione dell'impatto della violazione. Supporto nella gestione delle violazioni.
Segretario Generale	Coordinamento operativo del Comitato. Supporto nella valutazione delle conseguenze legali delle violazioni.
Responsabile Ufficio CED (solo nel caso di violazione per via informatica o telematica)	Supporto nella gestione della violazione
Responsabile apicale dell'ufficio coinvolto dalla violazione	Supporto nella analisi delle segnalazioni e gestione delle violazioni. Mettere a disposizione del Comitato l'elenco aggiornato dei fornitori più critici per la gestione dei dati personali.

Segnalazione di possibili violazioni

I destinatari della presente Procedura devono segnalare al Comitato le situazioni che potrebbero comportare una violazione di dati personali. Chi intercetta una situazione che potrebbe comportare una violazione di dati personali, deve tempestivamente informarne il Responsabile apicale della propria unità organizzativa o, in caso di sua assenza o indisponibilità, un altro componente del Comitato.

Il segnalatore è tenuto a collaborare col Comitato, fornendo tutti i dettagli utili alla valutazione del caso. Le modalità di raccolta delle segnalazioni sono descritte nel successivo paragrafo "raccolta delle segnalazioni".

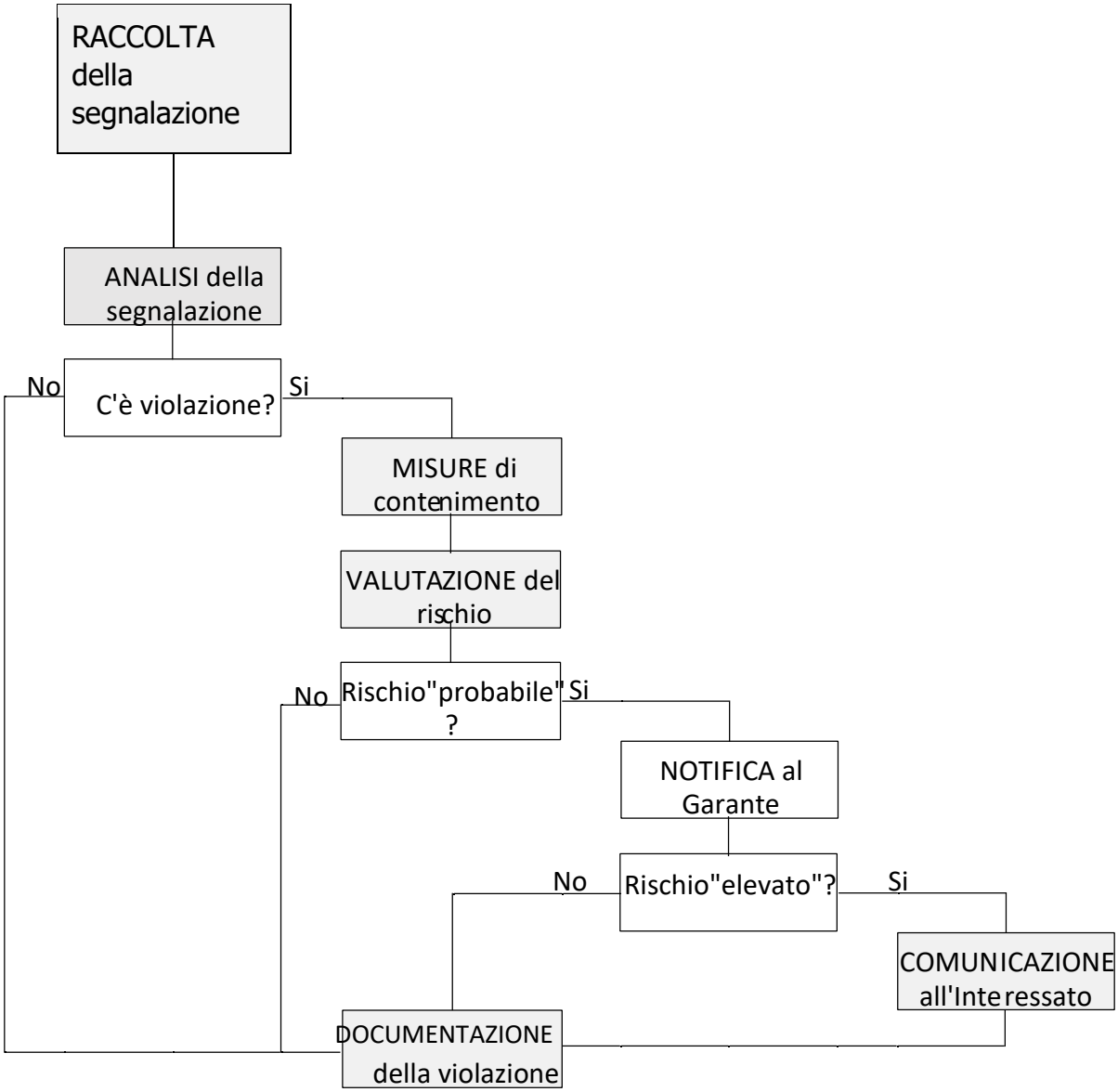
Tutti i dipendenti e collaboratori dell'Ente che accedono alle risorse del Sistema Informatico Informativo dell'Ente sono tenuti ad osservare i principi contenuti nel presente documento ed a segnalare in modo tempestivo la presenza di condizioni che possano indurre a valutare delle anomalie riconducibili ad attacchi informatici oppure a comportamenti scorretti.

Segnalazioni esterne - Data Breach presso un responsabile esterno del trattamento

Il soggetto che agisce in qualità di Responsabile esterno delle attività di trattamento per conto e nell'interesse del Comune di Porto Sant'Elpidio, deve informare l'Ente della violazione dei dati personali, senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui ne ha conoscenza, compilando il modulo online https://servizio.comune.portosantelpidio.fm.it/rwe2/module_preview.jsp?MODULE_TAG=segnalazione_data_breach
(o in alternativa utilizzare il modulo in allegato al presente documento).
Successivamente il Responsabile è tenuto a fornire al Comune tutta la collaborazione necessaria per consentirgli di adempiere agli obblighi previsti dalla normativa in materia di data breach.

Gestione del data breach

Viene di seguito rappresentato l'iter da seguire nella gestione del data breach



Raccolta della segnalazione

Chi, nel trattare dati personali di cui è titolare il Comune di Porto Sant'Elpidio, viene a conoscenza di eventi anomali che possano determinare la violazione di dati stessi, è tenuto a segnalarlo tempestivamente e comunque entro le 24 ore dal momento in cui ne viene a conoscenza, **al Responsabile apicale della propria unità organizzativa** compilando il modulo online https://servizio.comune.portosantelpidio.fm.it/rwe2/module_preview.jsp?MODULE_TAG=segnalazione_data_breach

In alternativa, è possibile utilizzare il modulo di segnalazione allegato al presente documento.

La segnalazione può provenire:

- da dipendenti del Comune e, in genere, da tutti i soggetti a qualunque titolo autorizzati ad accedere ad archivi e documenti cartacei, alla rete comunale e ai sistemi informatici del Comune di Porto Sant'Elpidio;
- dal Responsabile esterno del trattamento.

La segnalazione può altresì provenire da soggetti esterni (es. interessati).

Ricevuta una segnalazione, il membro del Comitato che l'ha ricevuta avvisa gli altri membri del Comitato.

Analisi della segnalazione e valutazione dell'evento

Il Comitato effettua un'analisi preliminare della segnalazione e sulla base delle informazioni raccolte, verifica se c'è stata violazione dei dati personali.

Qualora l'evento segnalato non costituisca violazione dei dati personali, la relativa motivazione viene riportata nel registro delle violazioni gestito attraverso la piattaforma in uso presso l'Ente.

Nel caso si accerti l'esistenza di una violazione di dati personali, si attivano le misure di contenimento e vengono esaminate le circostanze specifiche della violazione stessa per valutarne la gravità, stabilendo, in primo luogo, il tipo di violazione:

- Violazione di confidenzialità (divulgazione o accesso non autorizzato o accidentale ai dati);
- violazione dell'integrità (alterazione non autorizzata o accidentale dei dati);
- violazione della disponibilità (accidentale o non autorizzata perdita di accesso o distruzione dei dati personali).

Misure di contenimento

Appurato l'accadimento di una violazione, il Comitato attiva le prime misure di contenimento con l'obiettivo di ridurre il rischio per gli Interessati.

La tempestiva esecuzione di queste misure può significativamente incidere positivamente sull'esito finale della gestione del caso, evitando ad esempio la necessità di Comunicazione agli Interessati (cfr. Art.34 comma 3 lettera c: "*il titolare [adotta] misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati")*.

Esempi di misure di contenimento sono: il blocco o reset degli account violati da un furto di password; il recupero da backup di dati bloccati da un ransomware; l'oscuramento dal sito istituzionale di dati erroneamente pubblicati.

Valutazione del rischio

In una prima fase della valutazione del rischio deve essere stabilita la gravità dell'incidente di sicurezza.

Il livello di rischio, in relazione alla gravità del rischio e alla probabilità che il rischio si verifichi, può essere:

Livello di rischio	Descrizione
Alto	Il grado di compromissione di servizi e/o sistemi è elevato. Si rilevano danni consistenti sugli asset. Il ripristino è di medio o lungo periodo. L'incidente presenta una tra le seguenti condizioni: ● Danni a persone e rilevanti perdite di produttività. ● Compromissione di sistemi o di reti in grado di permettere accessi incontrollati a informazioni confidenziali. ● Siti web violati o utilizzati a fini di propagazione di materiale terroristico o pornografico. ● Frode o attività criminale che coinvolga servizi forniti dall'ente. ● Impossibilità tecnica di fornire uno o più servizi critici a un elevato numero di utenti per un intervallo di tempo superiore ai 30 minuti nell'arco di una giornata. ● Impossibilità tecnica di fornire uno o più servizi di criticità media per un periodo di tempo superiore ai 2 giorni lavorativi. ● Significativa perdita economica, di immagine e/o reputazione nei confronti del pubblico o degli utenti.
Medio	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta". Il grado di compromissione di servizi e/o sistemi è di una certa rilevanza e possono essere rilevati danni sugli asset di una certa consistenza. Il ripristino ha tempi che non compromettono la continuità del servizio L'incidente presenta una tra le seguenti condizioni: ● Compromissione di server. ● Degrado di prestazioni relativo ai servizi offerti dall'ente con conseguente perdita di produttività da parte degli utilizzatori. ● Attacchi che provocano il funzionamento parziale o intermittente della rete. ● Impossibilità tecnica di fornire uno o più servizi critici ad un elevato numero di utenti per intervalli di tempo inferiori ai 30 minuti di tempo ripetuti su più giornate. ● Impossibilità tecnica di fornire uno o più servizi critici ad una piccola parte di utenti per un periodo di tempo superiore ai 30 minuti di tempo nell'arco di una o più giornate. ● Basso impatto in termini di perdita economica, di immagine e/o reputazione nei confronti degli utenti.

Basso	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta o media". Non vengono compromessi asset o servizi. L'incidente presenta le seguenti condizioni: ● Interruzione dell'attività lavorativa di un numero ristretto di dipendenti e per un breve periodo di tempo. ● Contaminazioni da virus in un medesimo sito ma comunque identificate dai sistemi anti-malware. ● Nessuna o limitata perdita di operatività o di business da parte di un ridotto numero di dipendenti.

Si procede successivamente alla valutazione dei rischi per i diritti e le libertà delle persone fisiche interessate, con particolare attenzione a fattori di rischio quali:

- *Carattere particolare dei dati* (idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, dati relativi alla salute o alla vita sessuale, o relative alla salute o alla vita sessuale, a condanne penali, a reati o relative misure di sicurezza, dati che riguardino valutazioni di aspetti personali quali il rendimento professionale, la situazione economica, gli interessi personali, la salute, il comportamento, l'ubicazione e gli spostamenti, al fine di creare o utilizzare profili personali);
- *Profilazione personale* (rendimento professionale, situazione economica, interessi personali, condizioni di salute, comportamento, ubicazione, spostamenti …)
- *Quantità dei dati personali compromessi dalla violazione*
- *Numero degli interessati*
- *Facilità di identificazione degli interessati*
- *Particolarità delle conseguenze per gli interessati (es. minori)*
- *Gravità delle conseguenze per gli interessati (* ad esempio occorre valutare se i dati sono nella disponibilità di persone sconosciute o di persone conosciute, dalle quali il titolare può ragionevolmente aspettarsi che non li leggerà e rispetterà le istruzioni per restituirli. Si deve altresì tener conto della permanenza o della temporaneità delle conseguenze ai potenziali effetti negativi per gli interessati quali:
- *Discriminazioni, Furto o usurpazione di identità, Perdite finanziarie, Pregiudizio alla reputazione, Conoscenza da parte di terzi non autorizzati, Perdita di riservatezza di dati personali protetti da segreto d'ufficio, Decifratura non autorizzata della pseudonomizzazione, Danno economico o sociale significativo, Privazione o limitazione di diritti o di libertà, Impossibilità dell'interessato di esercitare i propri diritti sul trattamento dei suoi dati personali, Danni fisici, materiali o immateriali, alle persone fisiche*

Saranno inoltre valutate, come variabili qualitative dell'impatto temuto, le seguenti eventuali condizioni:

a) che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
b) che si tratti di dati relativi a valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le

preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;

c) che si tratti di dati di persone fisiche vulnerabili, in particolare minori;

d) che il trattamento riguardi una notevole quantità di Dati Personali;

e) che il trattamento riguardi un vasto numero di interessati.

Notifica all' Autorità Garante

Appurato che la violazione comporta "*un rischio per i diritti e le libertà della persona fisica dell'interessato*" (Art. 33 comma 1), il Comitato compila l'apposito modulo disponibile sul sito del Garante.

La violazione di dati personali deve essere notificata dal Titolare all'Autorità Garante (Garante della privacy), senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il Titolare ne è venuto a conoscenza.

Si considera che il Titolare sia a conoscenza della violazione nel momento in cui è messo al corrente del fatto che si è verificato un incidente di sicurezza che ha portato alla violazione di dati personali. Il momento esatto dipenderà dalle circostanze: in alcuni casi la violazione potrà essere evidente fin dall'inizio, in altri casi potrebbe essere necessario del tempo per stabilire se i dati personali siano stati compromessi.

E' importante porre l'accento sulla tempestività con cui deve essere effettuata l'indagine sull'incidente al fine di stabilire se c'è stata violazione dei dati personali e, in caso affermativo, prendere le misure adeguate ed effettuare, se necessario, la notifica.

Se si superano le 72 ore, la notifica deve essere corredata dalle ragioni del ritardo.

Vanno notificate unicamente le violazioni di dati personali che possono avere effetti avversi significativi sulla libertà e sui diritti degli interessati, causando danni fisici materiali o immateriali. Non è soggetta a notifica la violazione se si è in grado di dimostrare che è improbabile che la violazione stessa presenti un rischio per i diritti e le libertà delle persone fisiche (ad esempio, la divulgazione di dati personali già oggetto di pubblicazione). Se si considera probabile il rischio relativo alla violazione di dati personali sensibili, di salute o giudiziari o in caso di dubbio è più prudente effettuare la notifica.

Occorre tener presente che, anche qualora inizialmente la notifica non venga effettuata perché si valuta che non esista un rischio probabile per i diritti e le libertà delle persone fisiche, nel caso in cui la situazione cambi nel corso del tempo, occorre rivalutare il rischio e procedere eventualmente alla notifica.

La notifica viene inviata dal Titolare all'indirizzo protocollo@pec.gpdp.it utilizzando l'apposito modello predisposto dal garante, con firma digitale o allegando la fotocopia della carta di identità del firmatario. L'oggetto del messaggio deve necessariamente portare la dicitura " Notifica violazione dati personali " e opzionalmente la denominazione del titolare del trattamento

Se non è possibile fornire all'Autorità Garante, contestualmente alla notifica, tutte le informazioni richieste, il Titolare potrà informare quest'ultimo, indicandone le motivazioni, che non dispone ancora di tutte le informazioni e che fornirà ulteriori dettagli in un momento successivo, senza ingiustificato ritardo, non appena questi saranno disponibili.

Comunicazione agli interessati

Qualora la valutazione evidenzi un "*rischio elevato*" per le libertà ed i diritti degli Interessati, il GDPR richiede una Comunicazione ai singoli Interessati che descrive (art. 34 comma 2) "*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)" e cioè:

- nome e 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 dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Col supporto del Comitato, il Titolare o suo sostituto verifica se si ricade in uno dei casi elencati dall'Art. 34 comma 3 che esclude l'obbligo di Comunicazione ai singoli Interessati:

*"Non è richiesta la comunicazione all'interessato se è soddisfatta **una** delle seguenti condizioni:*

a) *il titolare ha messo in atto misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;*
b) *il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;*
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."*

Quindi:

- **se non si ricade in nessuno dei tre casi**, è richiesta una Comunicazione ai singoli Interessati
- **se si ricade nel caso c),** la Comunicazione ai singoli Interessati è sostituita da una Comunicazione pubblica, realizzabile con un avviso sul sito internet dell'Ente, di visibilità e durata con "analoga efficacia" della Comunicazione ai singoli Interessati
- **se si ricade nel caso a) e b)** non è richiesta alcuna Comunicazione.

Prima di procedere alla Comunicazione (singola o pubblica), il Titolare o suo sostituto (o in loro assenza il Responsabile apicale che ha provveduto alla valutazione) contatta il Garante per un confronto su necessità e tempi della Comunicazione.

In tutte e tre i casi, il Comitato provvede a riportare l'esito della valutazione nella Registrazione della violazione.

Documentazione della violazione

Le segnalazioni vengono conservate nel rispetto delle disposizioni del presente Manuale ovvero gestite telematicamente attraverso la piattaforma in uso.

Per ogni violazione segnalata, il Titolare, compila il Registro delle violazioni.

Ad integrazione di quanto riportato nel Registro, il DPO raccoglie e conserva presso le cartelle condivise del Comune di Porto Sant'Elpidio la scheda Evento, la scheda Violazione, l'eventuale notifica all'Autorità Garante, la comunicazione agli interessati e tutti i documenti relativi ad ogni segnalazione, compresi quelli inerenti le circostanze dell'evento, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione è resa disponibile all'Autorità Garante per le verifiche di competenza.

Segnalazione Data Breach al Comune di Porto Sant'Elpidio

Nome	
Cognome	
Codice Fiscale	
Email	
Telefono	

Data scoperta violazione:	
Data dell'incidente:	
Luogo della violazione (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili):	
Cognome e Nome, ruolo e dati di contatto della persona che ha rilevato/ riferito della violazione: indirizzo e-mail, numero telefonico): In caso di destinatario esterno indicare la ragione sociale:	
Denominazione della/e banca/ che dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati:	
Natura e tipo dei dati trattati:	
Supporto dei dati:	**|_| Fisico: cartaceo |_| Digitale |_| Altro**
Categorie e numero approssimativo di interessati coinvolti nella violazione	
Effetti e conseguenze della violazione	
Breve descrizione di eventuali azioni poste in essere al momento della scoperta della violazione:	
Necessità d'informare altri soggetti della violazione	

N.B: firmare digitalmente oppure firmare in modalità cartacea ma allegare copia di un documento di riconoscimento

Inviare tempestivamente la presente via pec alla casella pseprotocollo@postecert.elpinet.it oppure consegnare a mano all'Ufficio Protocollo del Comune di Porto Sant'Elpidio in Via Umberto Primo 485.