DISPOSIZIONI OPERATIVE IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONE DI DATI PERSONALI (c.d. DATA BREACH)

ENTE DI GESTIONE DELLE AREE PROTETTE DELLE ALPI MARITTIME

Piano approvato con Decreto Commissariale n. 14 del 2 aprile 2025

Sommario

FINALITÀ E AMBITO DI APPLICAZIONE

Il Titolare del trattamento è tenuto a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (di seguito, per comodità, "data breach"), incluse eventuali notifiche all'Autorità di controllo competente ed eventuali comunicazioni agli interessati.

Il mancato rispetto dell'obbligo di notifica ex art. 33 del RGPD comporta l'applicabilità da parte dell'autorità di controllo delle sanzioni amministrative previste dall'art. 83 del RGPD. **L'autorità potrebbe inoltre applicare le misure correttive previste dall'art. 58 del RGPD e, quindi, rivolgere al Titolare avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti provvisori o definiti al trattamento e di divieti, ordini di rettifica e cancellazione dei dati, revoche di certificazioni, ordini di sospendere i flussi di dati verso paesi terzi o organizzazioni internazionali**.

Il RGPD prevede poi espressamente che al momento della decisione in merito alla sanzione amministrativa pecuniaria da infliggere ed alla definizione del suo ammontare, è necessario tenere conto nel caso concreto anche delle misure adottate dal Titolare per attenuare il danno subito dagli interessati, come pure del grado di responsabilità del Titolare (o del responsabile) alla luce delle misure tecniche e organizzative messe in atto ai sensi degli artt. 25 e 32. La stessa mancata notifica all'autorità di controllo, e/o comunicazione all'Interessato, potrebbero d'altro canto essere considerate nel caso specifico indici di una mancata adozione di misure di sicurezza che potrebbe portare all'irrogazione di specifiche sanzioni al riguardo.

Inoltre, **l'art. 82 del RGPD prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del RGPD ha il diritto di ottenere il risarcimento del danno dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile)**.

È pertanto di fondamentale importanza predisporre una procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l'Ente (data breach policy). A tale riguardo si precisa che, presso il Titolare del trattamento, sono state attivate procedure a tutela della sicurezza dei dati, tra cui:

- l'adozione di misure organizzative e tecniche per garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati personali e alle altre informazioni trattate, comprese misure volte al tempestivo ripristino della disponibilità in caso di incidente sulla sicurezza;
- l'organizzazione, a cadenza periodica, di corsi di formazione per i dipendenti/collaboratori sui principi cardine della normativa sul trattamento dati, sulla sicurezza dei dati personali e dei sistemi.

I dati oggetto di riferimento sono i dati personali trattati "*da* "e "*per conto*" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo.

Il presente documento ha lo scopo di **indicare le modalità di gestione di un data breach, ovvero di un episodio di violazione di dati personali (come meglio spiegato nel prosieguo), nel rispetto dei principi e delle dispos**izioni contenute nel Regolamento (UE) 679/2016 sulla protezione dei dati personali (RGPD).

L'obiettivo del presente documento è, pertanto:

- sensibilizzare il personale in ordine alle responsabilità in materia di protezione dei dati personali ed all'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli incidenti sulla sicurezza (inclusi i data breach);
- definire processi per identificare, tracciare e reagire ad un incidente sulla sicurezza e ad un data breach, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di data breach, si renda necessario procedere alla (i) notifica al Garante e (ii) comunicazione agli Interessati;
- definire ruoli e responsabilità per la risposta agli incidenti sulla sicurezza ed i data breach;
- assicurare un adeguato flusso comunicativo all'interno della struttura del Titolare del trattamento, tra le figure coinvolte.

Le procedure qui contemplate sono applicabili a tutte le attività svolte dal Titolare del trattamento, con particolare riferimento alla gestione di tutti gli archivi e documenti cartacei e di tutti i sistemi informatici, attraverso i quali vengono trattati dati personali degli interessati, anche con il supporto di soggetti esterni.

Le procedure descritte nel presente documento sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento, quali:

a) i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto contrattuale intercorrente - abbiano accesso ai dati personali trattati nel corso delle prestazioni rese all'interno della struttura organizzativa comunale;
b) qualsiasi soggetto (persona fisica o persona giuridica) diverso da quelli indicati alla lettera precedente che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 del RGPD). In particolare, ogniqualvolta il Titolare del trattamento si trovi ad affidare il trattamento di dati ad un soggetto terzo, in qualità di responsabile del trattamento, è tenuto a stipulare con tale soggetto uno specifico accordo che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di data breach sia inclusa nel suddetto accordo. Ciò al fine di obbligare il responsabile ad informare il Titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di data breach;

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e **la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia**.

In questo documento si sintetizzano le regole per garantire la realizzabilità tecnica e la sostenibilità organizzativa nella gestione del data breach, sotto i diversi aspetti relativi a:

- modalità e profili di segnalazione al Titolare del trattamento;
- valutazione dell'evento accaduto;
- modalità e profili di notificazione all'Autorità di controllo;
- eventuale comunicazione agli interessati

garantendo al tempo stesso:

- 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.

Le disposizioni contenute nel presente documento sono applicabili, in quanto compatibili, anche in relazione alle violazioni di dati personali verificatesi nel contesto delle attività di trattamento dei dati personali che il Titolare del trattamento svolga in quanto **Autorità competente a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, in conformità alle previsioni di cui al Decreto Legislativo 18 maggio 2018, n. 51**.

Art. 26 del D.Lgs. 51/2018:
"*1. Salvo quanto previsto dall'art. 37, comma 6, in caso di violazione di dati personali, il titolare del trattamento notifica la violazione al Garante con le modalità di cui all'art. 33 del regolamento UE.*
2. Se la violazione dei dati personali riguarda dati personali che sono stati trasmessi dal o al titolare del trattamento di un altro Stato membro, le informazioni previste dal citato art. 33 del regolamento UE sono comunicate, senza ingiustificato ritardo, al titolare del trattamento di tale Stato membro."
Art. 27 del D.Lgs. 51/2018:
"*1. Quando la violazione di dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, si osservano le disposizioni in tema di comunicazioni di cui all'art. 34 del regolamento UE.*
2. La comunicazione all'interessato di cui al comma 1 può essere ritardata, limitata od omessa alle condizioni e per i motivi di cui all'art. 14, comma 2."

DEFINIZIONI

Fermo restando che le uniche definizioni "ufficiali" e vincolanti sono quelle contenute nell'art. 4 del RGPD e quelle contenute nel Codice per la protezione dei dati personali (D.Lgs. 30 giugno 2003 n. 196), si riporta la terminologia maggiormente utilizzata nel contesto del presente documento, per semplificarne la lettura.

«**GDPR**» o «**RGPD**» o «**Regolamento**»: il Regolamento (UE) n. 679/2016 "General Data Protection Regulation", in italiano indicato come "Regolamento generale sulla protezione dei dati";

«**CODICE PRIVACY**»: il Decreto Legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali";

«**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;

«**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, nonché trattare 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;

«**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;

«**DATI GENETICI**»: 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 BIOMETRICI**»: 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;

«**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;

«**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;

«**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;

«**COMUNICAZIONE**»: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'Interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'art. 2-quaterdecies del Codice privacy, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

«**DIFFUSIONE**»: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

«**INTERESSATO**»: la persona fisica cui si riferiscono i dati personali;

«**TITOLARE DEL TRATTAMENTO**»: 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**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

«**RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI**» o «**RPD**» o «**RPD**»: soggetto cui è attribuito dal Titolare del trattamento il compito di informare e fornire

consulenza sugli obblighi derivanti dal RGPD e di sorvegliarne l'osservanza. Fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati (PIA) e ne sorveglia lo svolgimento. Coopera con l'Autorità di controllo e funge da punto di contatto con essa (RGPD, art. 37, 38, 39);

«**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;

«**MINACCIA**»: una serie di eventi dannosi che possono compromettere le caratteristiche di integrità, riservatezza e disponibilità del dato personale;

«**DANNO**»: conseguenza negativa derivante dal verificarsi di una determinata minaccia; il danno può qualificarsi come materiale quando determina una concreta lesione all'ambito fisico o patrimoniale dell'Interessato oppure immateriale quando riguarda le possibili conseguenze dannose derivanti dal trattamento di dati personali, di natura non patrimoniale e che affliggono la sfera interiore del soggetto Interessato;

«**MALWARE**»: software di tipo malevolo che causa danni ai sistemi informativi;

«**MISURA DI SICUREZZA**»: accorgimento tecnico e organizzativo utilizzato per garantire che i dati non vadano distrutti o persi anche in modo accidentale, per garantire che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti;

«**CRITTOGRAFIA**»: tecnica che permette di "cifrare" un messaggio rendendolo incomprensibile a tutti fuorché al suo destinatario;

«**DECRITTOGRAFIA**»: il processo per "sbloccare" i dati criptati, cioè cifrati;

«**AUTORITÀ DI CONTROLLO**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 del RGPD. In Italia, il Garante per la Protezione dei Dati Personali;

«**WP ART. 29**»: gruppo di lavoro indipendente con funzioni consultive dell'UE nell'ambito della protezione dei dati personali e della vita privata, istituito ai sensi dell'art. 29 della direttiva 95/45/CE. A decorrere dal 25 maggio 2018 è stato sostituito dal Comitato europeo per la protezione dei dati (EDPB) ai sensi del regolamento generale sulla protezione dei dati dell'UE (RGPD) (regolamento (UE) 2016/679);

«**EDPB**» o «**EUROPEAN DATA PROTECTION BOARD**»: Il Comitato europeo per la protezione dei dati (EDPB) è un organismo europeo indipendente. È l'organizzazione sotto la cui egida si riuniscono le Autorità nazionali per la protezione dei dati personali (Autorità nazionali di controllo) dei paesi dello Spazio economico europeo, nonché il Garante europeo della protezione dei dati (EDPS). L'EDPB garantisce che il Regolamento generale sulla protezione dei dati e la Direttiva "polizia e giustizia" siano applicati in modo coerente; inoltre, l'EDPB garantisce la cooperazione, anche in materia di attuazione della normativa;

«**LINEE GUIDA**»: con questo termine si intende riferirsi al documento denominato "*Linee guida 9/2022 sulla notifica di violazione dei dati personali ai sensi del GDPR*", versione 2.0, adottato dall'EDPB in data 28 marzo 2023[1]. Si ricorda, tuttavia, che il Gruppo di lavoro ex art. 29 ("WP29") ha adottato il 6 febbraio 2018 la versione definitiva delle linee guida sulla notifica delle violazioni dei dati personali (cd. "data breach") ai sensi del Regolamento UE n. 679/2016 (cd. "RGPD")[2]. Durante la prima riunione plenaria del 25/05/2018 il Comitato europeo per la protezione dei dati aveva approvato le linee-guida relative al regolamento generale sulla protezione dei dati messe a punto dal gruppo di lavoro "Art. 29"[3].

Successivamente, in data 14 dicembre 2021, l'EDPB ha pubblicato le "*Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali*"[4]. Tale testo (**ALLEGATO F** al presente documento) mantiene la propria utilità quanto alle fattispecie esemplificative elencate.

PIANO DI AZIONE

È individuato il seguente piano d'azione per assicurare la conformità (compliance) del Titolare del trattamento alle previsioni normative in tema di protezione dei dati personali. Il piano evidenzia in rosso le azioni "obbligatorie" ed in giallo quelle "non obbligatorie ma, vivamente, consigliate". Trattasi ovviamente di **indicazioni di massima**, debitamente integrate dalle regole contenute nel prosieguo del documento, che sono suscettibili di modifica ed integrazione in considerazione dell'evoluzione normativa e tecnica e delle peculiari caratteristiche organizzative del Titolare del trattamento.

Azione	Annotazioni
Adottare una procedura interna di gestione dei data breach (obbligatorio)	Attraverso la presente policy sono definiti i ruoli e le responsabilità nella gestione degli incidenti e delle violazioni
Istruire il personale autorizzato al trattamento dei dati in materia di sicurezza e gestione di possibili violazioni (obbligatorio)	Il personale dev'essere in grado di identificare e gestire eventuali violazioni di dati personali
Verificare lo stato delle misure di sicurezza implementate presso l'Ente (consigliato)	Condurre audit sui sistemi informatici e non. Il RGPD richiede infatti che siano implementate tutte le misure

[1] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_it.
[2] Linee guida WP29 sulla notifica di violazione dei dati personali ai sensi del regolamento 2016/679 (WP250 rev.01) (ultima revisione e aggiornamento il 6 febbraio 2018), disponibile all'indirizzo https://ec.europa.eu/newsroom/article29/items/612052.
[3] https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.
[4] https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_it.pdf

	tecnologiche ed organizzative per valutare se sia avvenuta una violazione di dati; tali misure aiutano anche a stabilire se sia necessaria o meno la notifica
Cifrare o pseudonimizzare i dati di cui agli articoli 9 e 10 del RGPD (obbligatorio)	
Limitare l'accesso ai dati personali solo al personale autorizzato (obbligatorio)	È opportuno limitare l'accesso per ridurre le possibilità di eventuali violazioni, che spesso sono provocate anche da errore umano
Verificare le misure di sicurezza installate sui computer al fine di eliminare le vulnerabilità ed implementare misure di sicurezza logiche e fisiche adeguate (obbligatorio)	Occorre valutare le misure di sicurezza anche al fine di dimostrare la c.d. "accountability"
Preparare un piano di risposta alle violazioni (obbligatorio)	Il piano dovrebbe prevedere le seguenti azioni: – assicurare che i dati non siano più compressi; – mettere in sicurezza tutti i dati ed i sistemi; – identificare i dati compromessi, le categorie di Interessati coinvolte, la tipologia di violazione; – isolare i dati compromessi; – modificare le chiavi di codifica e le relative password immediatamente; – documentare tutte le fasi di gestione della violazione e tutte le informazioni relative alla violazione stessa; – determinare quando sia effettivamente avvenuta la violazione (al fine di notificare la violazione entro 72 ore)
Coinvolgere le autorità competenti ove si sospettino attività illecite (obbligatorio)	Non è strettamente richiesto dal RGPD, ma è opportuno notificare la violazione anche ad altre autorità, ove applicabile e richiesto dalla normativa vigente
Selezionare adeguatamente i fornitori che erogano attività che comportano un trattamento di dati (obbligatorio)	È opportuno verificare e selezionare il fornitore e assicurare che la designazione come Responsabile contenga previsioni e istruzioni specifiche in materia di data breach
Conclusa la gestione urgente della violazione, valutare i "gaps" e l'efficacia dei sistemi interni, della formazione del personale e delle ulteriori procedure che mirano a tutelare i dati personali (obbligatorio)	Tale attività potrebbe essere inclusa in una fase di post-assessment
Testare frequentemente i sistemi interni (consigliato)	

Conservare un registro dei data breach ed aggiornarlo frequentemente (obbligatorio)	Il Titolare è tenuto a comunicare ogni informazione sulla violazione all'Autorità di controllo e per tale motivo è opportuno implementare un registro di data breach

PROCEDURA

Considerando 85, del RGPD:

"*Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.*"

Si individuano di seguito i soggetti coinvolti ed il flusso delle principali attività previste per la rilevazione e gestione di un incidente di sicurezza che possa comportare una violazione di dati personali (si veda la rappresentazione grafica nell'ALLEGATO A).

La **tempestività** è un fattore determinante nella risposta agli incidenti sulla sicurezza ed ai data breach ed è dovere di ciascun soggetto, nell'ambito del proprio ruolo nella struttura e nella catena di comunicazione, non ritardare iniziative di reazione all'incidente e rispettare le procedure e le tempistiche di comunicazione individuate dal presente documento.

La risposta a un Incidente sulla sicurezza o ad un data breach deve avvenire secondo le fasi descritte di seguito. Considerando, tuttavia, che gli Incidenti possono avere molteplici cause o coinvolgere diversi soggetti ed avere conseguenze caratterizzate da vari livelli di gravità, tali fasi potrebbero sovrapporsi o richiedere tempistiche differenti o aggiornamenti. È tuttavia fatto obbligo ad ogni soggetto operante sotto la responsabilità del Titolare del trattamento di collaborare e seguire le istruzioni che di volta in volta gli vengano fornite dallo stesso Titolare del trattamento o dal RPD.

Considerati i rischi e, in caso di data breach, le ridotte tempistiche per effettuare la notifica e per la comunicazione agli interessati, occuparsi degli incidenti di sicurezza deve essere obiettivo prioritario per tutti i soggetti coinvolti nella loro gestione. Nella gestione di un qualunque incidente di sicurezza devono essere considerate le seguenti due priorità:
prima priorità: proteggere tutti gli assets del Titolare del trattamento, incluse le risorse colpite dall'incidente, fino al ripristino della normale operatività;
seconda priorità: raccogliere informazioni e prove per supportare le eventuali e appropriate azioni correttive, disciplinari o legali;

Tutti gli incidenti di sicurezza ed i data breach devono essere trattati con il **massimo livello di riservatezza**: le informazioni devono essere condivise esclusivamente con il personale identificato nella presente procedura e solo quando strettamente necessario. Eventuali comunicazioni a soggetti non coinvolti nella gestione dell'Incidente dovranno limitarsi all'indicazione che si è verificato un problema e che lo stesso è in fase di gestione.

Tutte le attività di gestione devono essere **tracciate e documentate** per quanto possibile a partire dall'istante di rilevazione.

Il coordinamento delle attività di gestione di una violazione di dati personali, con particolare riferimento agli obblighi di comunicazione e notifica imposti dal RGPD, è assicurato dal RPD con il supporto dell'Amministratore di sistema, ove presente, per gli aspetti tecnici e dal Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta. Il RPD ha, comunque, piena facoltà di suggerire la convocazione ed il coinvolgimento di altri soggetti che ritenga utili alle necessità del caso.

1. Individuazione della violazione

Art. 33, par. 1, del RGPD:
"*In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, 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*"
Art. 4, par. 1, n. 2, del RGPD:
"*Ai fini del presente regolamento s'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"
Considerando 87 del RGPD:
"*È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato.*"

Le violazioni dei dati personali sono una tipologia di incidente per la sicurezza delle informazioni nel quale sia coinvolto qualsiasi genere di dato di natura personale (anagrafici, numeri di carte personali, codici identificativi, dati sanitari, dati biometrici, dati relativi a conti correnti, ecc.). **Tuttavia, come indicato all'art. 4, punto 12, il RGPD si applica soltanto in caso di violazione di dati personali**.

La conseguenza di tale violazione è che il Titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'art. 5 del RGPD. Questo punto mette in luce la differenza tra un incidente di sicurezza e una violazione dei dati personali: mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.

Non è da ritenersi corretta la comune associazione tra data breach ed attacco o problema informatico poiché tale violazione può avvenire anche (ad esempio) a causa di un dipendente infedele che sottragga documentazione cartacea ovvero un di dipendente disattento che la smarrisca.

Le violazioni dei dati personali sono, di per sé, problematiche, ma possono anche essere sintomi di un regime di sicurezza dei dati vulnerabile e forse obsoleto, oppure segnalare carenze del sistema, da affrontare. In linea generale, è sempre meglio prevenire le violazioni dei dati preparandosi in anticipo, dal momento che diverse conseguenze sono per loro natura irreversibili. Prima che il Titolare del trattamento possa valutare appieno il rischio derivante da una violazione causata da una qualche forma di attacco, occorre individuare la causa alla radice del problema, al fine di stabilire se le vulnerabilità che hanno determinato l'incidente siano ancora presenti e siano pertanto ancora sfruttabili.

Le Linee Guida precisano la nozione di violazione in base ai seguenti **tre principi di sicurezza delle informazioni**:

Violazione della riservatezza *(Confidentiality breach)*	**divulgazione o accesso non autorizzato o accidentale** ai dati personali come, ad esempio: • quando nella redazione di un atto non si redige la versione con omissione dei dati da non pubblicare e l'atto viene pubblicato nella sua interezza; • quando si inoltrano messaggi contenenti dati a soggetti non interessati al trattamento; • quando un operatore abbandona la propria postazione di lavoro senza prima prendere le opportune precauzioni (riporre la documentazione, lasciare attive procedure sulla risorsa informatica utilizzata, ecc..) e terze persone prendono visione di informazioni; • quando un soggetto in malafede comunica dei dati non pubblici a terzi in modo non autorizzato. Per "**divulgazione**" si intende la trasmissione non autorizzata o impropria dei dati personali degli interessati verso terze parti (persone fisiche, persone giuridiche, gruppi di soggetti, pubblico) anche non precisamente identificabili. Per "**accesso**" si intende l'accesso non autorizzato o improprio ai dati degli interessati. Accessi ai dati (anche in sola visualizzazione, sia in caso di accessi logici ai sistemi informatici sia agli archivi cartacei) effettivamente avvenuti al di fuori dei processi operativi di trattamento dei dati previsti e autorizzati. Un **trattamento non autorizzato o illecito** può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del RGPD.

Violazione dell'integrità *(Integrity breach)*	**alterazione non autorizzata o accidentale** dei dati personali La "***alterazione***" è la situazione in cui i dati sono danneggiati, corrotti o non più completi. L'alterazione non autorizzata può essere la conseguenza di un attacco esterno o di una manipolazione inconsapevole da parte di personale non competente. Un'alterazione accidentale si può verificare per errore umano (ad es. nel momento di un aggiornamento delle informazioni) o per un disguido tecnico quando all'interno di una base dati si perdono i collegamenti a determinate informazioni (integrità referenziale).

Violazione della disponibilità *(Availability breach)*	**accidentale o non autorizzata perdita di accesso** o **distruzione** di dati personali (Fattispecie non sempre di facile individuazione). La "***perdita di dati***" è la situazione in cui i dati, presumibilmente, esistono ancora, ma il Titolare ne ha perso il controllo o la possibilità di accedervi. Perdita del supporto fisico di memorizzazione dei dati (dischi esterni, pendrive ecc.) in termini di privazione, sottrazione, smarrimento dei dispositivi contenenti i dati degli interessati oppure dei documenti cartacei. La perdita può essere anche temporanea ma superiore ad un termine ragionevole. Può riguardare le copie o gli originali dei supporti contenenti i dati personali dei soggetti interessati. La "***distruzione***" dei dati personali è la condizione in cui i dati non esistono più o non esistono più in un formato che sia utilizzabile dal Titolare. La violazione può essere determinata da una eliminazione logica (es. cancellazione dei dati) oppure fisica (es. rottura dei supporti di memorizzazione) non autorizzata e relativa impossibilità di ripristinare i dati entro un termine ragionevole. Ci sarà sempre una violazione della Disponibilità del dato nel caso di **perdita o distruzione permanente** dei dati. L'indisponibilità dei dati è quindi da considerare una violazione quando potrebbe avere un impatto significativo sui diritti e le libertà delle persone fisiche. Non si tratta invece di una violazione quando l'indisponibilità è dovuta a interruzioni programmate per la manutenzione).

	Ci si potrebbe chiedere se una **perdita temporanea della disponibilità** dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica. L'art. 32 del RGPD ("Sicurezza del trattamento") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "*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*". Di conseguenza, un incidente di sicurezza che determini l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza" ai sensi dell'art. 4, n. 12 del RGPD. Va notato che, sebbene una perdita di disponibilità dei sistemi del Titolare del trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il Titolare consideri tutte le possibili conseguenze della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi.

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

La violazione dei dati può avvenire a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB, etc.) o per la sottrazione o perdita di documenti con dati personali (furto, smarrimento, abbandono, etc.). La casistica è molto ampia.

A mero **titolo esemplificativo** e senza pretesa di esaustività, l'oggetto della segnalazione di un data breach può essere:

- l'accesso abusivo (ad esempio: accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- dati cancellati accidentalmente o da soggetti non autorizzati;
- perdita della chiave di decriptazione;

- dati persi dall'ambiente di produzione che non possano essere ripristinati integralmente dalle copie di sicurezza e si debba provvedere manualmente alla loro ricostruzione;
- interruzione significativa di un servizio ("*black out*" elettrico o attacchi di tipo "*denial of service*");
- divulgazione di dati confidenziali a persone non autorizzate;
- errori nell'implementazione di una policy di controllo e verifica periodica delle abilitazioni degli accessi;
- divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato;
- pubblicazione erronea delle informazioni personali (non di dominio pubblico) sul portale web istituzionale del Titolare del trattamento;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- perdita o il furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o il furto di documenti cartacei;
- pirateria informatica;
- virus o altri attacchi al sistema informatico o alla rete dell'Ente;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "*owner*";
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- formattazione di dispositivi di memorizzazione;
- malfunzionamenti software quali esecuzione di uno script automatico non autorizzato; errori di programmazione che causano output errati, ecc.;
- distruzione dolosa dei documenti: ad esempio incendio doloso provocato da personale interno o soggetti esterni che rende indisponibile in modo definitivo i documenti contenenti dati personali;
- distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura e di elettricità, umidità, corto circuito, caduta accidentale, eventi catastrofici/incendi, ecc.;
- guasti alla rete informatica: a titolo di esempio caduta delle comunicazioni durante il trasferimento di dati e perdita di dati durante la trasmissione, ecc.;
- invio di e-mail contenenti dati personali e/o particolari ad erroneo destinatario.

2. Rilevazione della violazione

La prima fase nella gestione del data breach è quella che conduce alla rilevazione della violazione o presunta violazione di sicurezza e della sua comunicazione al **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta**. Nell'ipotesi in cui ci si dovesse accorgere di essere stati vittima di un data breach la prima cosa da fare è quella di **non farsi prendere dal panico ed agire in modo scomposto** ma, anzi, applicare subito le procedure previste dalla presente policy.

2.1. Acquisizione della notizia

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia **affrontata immediatamente e correttamente** al fine di minimizzare l'impatto della violazione e prevenire che si ripeta. Ai fini di una corretta analisi della segnalazione, è necessario raccogliere fatti concreti prima di segnalare qualsiasi tipo di violazione, illecito ed irregolarità in ambito di tutela dei dati personali.

È importante che la raccolta della segnalazione o l'esecuzione della segnalazione da parte degli uffici avvenga **raccogliendo quante più informazioni possibili** (identificazione dei segnalatori, data ed ora in cui la segnalazione è avvenuta, dati descrittivi sulla violazione segnalata ecc..). **Le segnalazioni, pertanto, devono essere fondate su elementi di fatto precisi, circostanziati e concordanti**.

Se al momento della rilevazione dell'incidente di sicurezza non è disponibile una descrizione particolareggiata dell'evento, è comunque essenziale procedere immediatamente alla comunicazione dell'incidente al **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta**, per una prima valutazione d'impatto, anche con **informazioni incomplete**. Laddove necessario, alla prima valutazione possono seguirne altre, in base alle informazioni che vengono acquisite nella prosecuzione dell'indagine.

2.2. Fonte della notizia

La segnalazione di un data breach può essere **interna** (da personale dipendente, convenzionato, stagisti, tirocinanti, amministratori, RPD, …) o **esterna all'Ente** (Agid, ACN, Polizia, altre Forze dell'Ordine, giornalisti, utenti di servizi, RPD, Responsabili del trattamento, ecc.). Inoltre, ogni **Interessato** può segnalare, anche solo in caso di sospetto, che i propri dati personali siano stati utilizzati abusivamente o fraudolentemente da un terzo; in tal caso, l'Interessato può richiedere al Titolare del trattamento la verifica dell'eventuale violazione.

Il pubblico e, in genere, i soggetti che non sono legati al Titolare del trattamento da rapporti contrattuali od altrimenti vincolanti, possono segnalare anomalie, disservizi o potenziali incidenti sulla sicurezza mediante comunicazione scritta inviata al protocollo. Il Titolare del trattamento rende disponibili presso i propri uffici e sul **sito web istituzionale**, la **modulistica** e le **informazioni** utili allo scopo. Sebbene la segnalazione possa avvenire in forma libera, si ritiene opportuno suggerire al segnalante l'utilizzo di un apposito modello **ALLEGATO B - "*Modulo di segnalazione di una potenziale violazione di dati personali*"**, predisposto in modo tale da agevolare l'attività istruttoria e valutativa da parte del Titolare del trattamento.

Nel caso in cui la segnalazione sia raccolta presso persone fisiche, senza l'utilizzo della modulistica e delle procedure di cui sopra, è opportuno che chi riceve la segnalazione provveda anche a raccogliere informazioni di contatto sul segnalante (indirizzo di reperibilità, numeri telefonici, indirizzo di posta elettronica) che potranno, nel caso, essere utili durante la fase di gestione tecnica, per reperire maggiori informazioni circa la violazione segnalata. Ove possibile è sempre opportuno invitare il segnalante a rendere la propria dichiarazione per iscritto, anche in forma libera. In questa fase è opportuno non raccogliere dati personali appartenenti alle categorie particolari di cui all'art. 9 del RGPD, se non strettamente necessari.

Qualora la segnalazione pervenisse per **posta elettronica** certificata od ordinaria su una casella qualsiasi (istituzionale o meno) non è sufficiente il solo inoltro del messaggio ma occorre, comunque, seguire le modalità di seguito riportate. Allo stesso modo, ove la segnalazione pervenisse su **supporto cartaceo** non è sufficiente la sua mera registrazione al protocollo, occorrendo comunque che si segua la procedura di cui *infra*. Questo per accertarsi che la segnalazione non passi inosservata.

Anche le **segnalazioni anonime e/o verbali** devono essere raccolte e trasmesse conformemente a quanto *infra*, al fine di accertare la reale sussistenza della violazione, disporre l'eventuale notifica o le comunicazioni ed assumere i provvedimenti atti ad evitare l'aggravamento della situazione.

La **segnalazione di una potenziale violazione di dati personali da parte del personale operante all'interno della struttura organizzativa del Titolare del trattamento** deve avvenire solamente utilizzando l'apposito modello **ALLEGATO B - "*Modulo di segnalazione di una potenziale violazione di dati personali*"**.

2.3. Il monitoraggio degli eventi di sicurezza con impatto sulla protezione dei dati personali

L'individuazione di potenziali violazioni dei dati personali può anche avvenire a seguito di **attività di monitoraggio** degli eventi che possono arrecare violazioni dei dati, sia digitale ed automatizzata che cartacea. Il monitoraggio viene effettuato tramite il controllo delle attività di trattamento definite nel Registro dei trattamenti, in particolare per quei trattamenti che sono stati valutati con rischio non trascurabile in fase di valutazione d'impatto.

Le attività di monitoraggio si possono suddividere in due tipologie:

A) Il monitoraggio degli eventi generati dai sistemi ICT: tale monitoraggio include l'insieme delle attività di controllo finalizzate al rilevamento degli eventi tracciati dai sistemi informatici e dalle infrastrutture di sicurezza perimetrale che assumono carattere di rilevanza ai fini della sicurezza informatica. Tali eventi relativi ai sistemi ICT sono monitorati e gestiti dall'Amministratore di sistema, ove presente, al quale è assegnato il compito di identificare le categorie di eventi che dovrebbero essere sottoposte a monitoraggio, sulla scorta della seguente elencazione (meramente esemplificativa):

- log generati dalle attività svolte con account riconducibili agli amministratori di sistema, con particolare attenzione a:
  - orari di connessione/disconnessione (log-on / log-off);
  - log afferenti alla gestione dei profili utente (es. creazione di nuove utenze, modifica dei privilegi di accesso, blocco di utenze, forzato cambio password, riassegnazione di account ad altro utente);
  - modifiche alle configurazioni di sistema;
  - escalation o tentata escalation a profili con privilegi di accesso superiori;
  - qualsiasi attività svolta da remoto al di fuori dei consueti orari di lavoro;
  - qualsiasi attività bloccata dalle misure di sicurezza e controllo accessi (es. accessi negati; user-id o password errata);
- log generati dalle attività svolte da utenti ordinari, con particolare attenzione a:
  - orari di connessione/disconnessione (log-on / log-off);
  - accessi negati;
  - escalation o tentata escalation a profili con privilegi di accesso superiori;
  - qualsiasi attività svolta da remoto al di fuori dei consueti orari di lavoro;
  - qualsiasi attività bloccata dalle misure di sicurezza e controllo accessi (es. accessi negati; user-id o password errata);
- log generati dai sistemi di sicurezza:
  - tentativi di violazione delle politiche di firewalling (es. drop/reject);
  - allarmi generati dai sistemi antivirus;
  - allarmi generati dai sistemi antispamming;
  - allarmi generati dai directory server/service.

B) Il monitoraggio dei luoghi fisici del trattamento e dell'archiviazione di dati personali. I luoghi fisici preposti al trattamento di informazioni personali riconducibili alle categorie di cui agli articoli 9 e 10 del RGPD, con particolare riferimento agli eventuali archivi cartacei, devono essere controllati periodicamente dal personale preposto alla vigilanza, ove previsto, ed anche con l'ausilio di eventuali dispositivi di videosorveglianza. In ogni caso sia il personale di guardiania o di vigilanza, sia il personale operativo, autorizzato all'accesso ai locali o al trattamento dei dati personali, è tenuto a comunicare tempestivamente qualsiasi evento di presunta o palese violazione della privacy come ad esempio:

- smarrimento o furto di documenti cartacei contenenti informazioni personali;
- smarrimento o furto di supporti digitali o di computer fissi o mobili contenenti dati personali;
- constatazione di effrazione o tentativi di effrazione alle porte di accesso od alle serrature di chiusura degli armadi che custodiscono documenti;
- presenza di personale non autorizzato nei locali preposti al trattamento di informazioni personali.

Qualunque constatazione di violazione o sospetta violazione, emersa in sede di monitoraggio, deve essere comunicata al **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta, senza ritardo**.

2.4. Trasmissione della notizia

Ricevuta, da chiunque ed in qualunque modo, la segnalazione di un potenziale od effettivo incidente sulla sicurezza, la medesima è immediatamente **trasmessa al Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta**, compilando il documento di cui all'**ALLEGATO C - "Modulo di inoltro di segnalazione di una potenziale violazione di dati personali"**, **senza ritardo**. Il modello di segnalazione, debitamente compilato e sottoscritto, dovrà essere consegnato con le modalità più idonee (posta elettronica, consegna a mani, …) a garantirne la pronta e puntuale conoscenza in quanto permetterà di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso e, ciò, al fine di stabilire se si sia effettivamente verificata un'ipotesi di data breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto. Contestualmente alla **trasmissione documentale** della segnalazione è necessario **l'avvertimento** del destinatario anche in modo **verbale** allo scopo di assicurarsi che quanto comunicato non passi inosservato.

Ricevuta la segnalazione, il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta**, provvedono ad **informarne prontamente e, comunque non oltre 12 ore dalla conoscenza della segnalazione, il RPD.**

Il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta**, anche insieme ai soggetti coinvolti nell'incidente e sotto la supervisione del RPD, coordinano la raccolta delle informazioni nel più breve tempo possibile.

3. Analisi e Valutazione della violazione

Questa fase si compone di tutte quelle operazioni, accertamenti e verifiche tese a supportare la valutazione dell'accaduto.

Una volta stabilito che un data breach è avvenuto, il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta, insieme al RPD ed all'Amministratore di sistema, ove presente**, dovranno stabilire:

a) se sia probabile o meno che la violazione dei dati personali presenti un **rischio per i diritti e le libertà delle persone fisiche**;

b) se esistano e quali siano le **misure efficaci** per contenere ed affrontare la violazione;
c) una volta identificate tali misure, quali siano i **soggetti che devono agire** per contenere ed affrontare la violazione;
d) se sia necessario **notificare** la violazione all'Autorità di controllo;
e) se sia necessario **comunicare** la violazione agli interessati.

Il Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta) sono responsabili, sulla base delle rispettive competenze ed in base alla tipologia della violazione, dell'analisi tecnica dell'evento e delle azioni da mettere in atto tempestivamente per il contenimento del danno.

È importante che questa fase, nella sua prima esecuzione, **si concluda nel più breve tempo possibile, massimo 24/48 ore**, per consentire il primo processo decisionale di valutazione da parte del **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta** e permettere loro di eseguire le eventuali notifiche e comunicazioni entro i termini previsti.

In questa fase, è fondamentale raccogliere il maggior numero di informazioni relative alla violazione di dati personali e, anche in caso queste non siano per il momento ritenute esaustive, effettuare comunque la notificazione all'Autorità di controllo. Si veda il successivo paragrafo 4.2.2. in ordine alla possibilità di effettuare la notifica all'Autorità di controllo "per fasi".

3.1. Analisi tecnica dell'evento

Per identificare le modalità di gestione di una violazione e gli eventuali obblighi di notifica e/o di comunicazione, il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta** (con il supporto dell'Area Technology Office od altra figura equivalente) effettuano, anzitutto, un'analisi tecnica della segnalazione, all'interno della quale, **dovrà essere accertato se la violazione segnalata sia considerabile o meno un data breach**.

Questa fase dev'essere condotta con **estrema celerità**, anche se non si riescono ad individuare tutti gli elementi utili, ad eccezione della determinazione della sussistenza della violazione. Le verifiche potranno eventualmente proseguire anche dopo una prima valutazione. Inoltre, l'Autorità di controllo o gli alti organi nazionali (polizia, magistratura, CSIRT Italia, CNAIPIC, ecc.) potrebbero richiedere o ritenere necessari approfondimenti. Dunque, l'incompletezza delle informazioni, così come la necessità di approfondimenti potrebbero rendere necessario ripetere la fase anche più volte.

Nessuna segnalazione deve concludersi in questa fase unicamente sulla base di un giudizio di inaffidabilità del segnalante: occorrerà comunque appurare se la violazione si sia effettivamente verificata. **Parimenti, nessuna segnalazione che sia relativa unicamente ad operazioni svolte con strumenti informatici potrà concludersi durante l'analisi tecnica per il solo fatto che non sussiste una violazione di dati personali, in quanto potrebbe in ogni caso rendersi necessario informare altre Autorità competenti (ad es., CSIRT Italia, CNAIPIC, ecc.)**.

Cons specifico riferimento agli incidenti di sicurezza "tecnologici" si dovranno, ove possibile, rilevare:
- la causa e la natura del disservizio, della rottura e, in generale, dell'incidente di sicurezza;

- le eventuali vulnerabilità collegate con l'incidente e le azioni di mitigazione delle vulnerabilità individuate;
- l'esistenza di misure adottate precedentemente all'evento per contrastare il rischio;
- la valutazione dei tempi e modalità di riparazione e ripristino dei sistemi, dell'infrastruttura e delle configurazioni;
- la verifica dei sistemi recuperati;
- l'eventualità di perdita di dati durante il ripristino, la loro tipologia, se i dati sono reperibili in altre aree dei sistemi o presso terzi e le tempistiche per il recupero.

3.2. Valutazione della violazione al fine del rispetto degli obblighi di notifica e comunicazione

Esaurita l'analisi tecnica, il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta**, dovranno svolgere tutte le operazioni necessarie a raccogliere gli elementi per l'ulteriore valutazione dell'evento, ai fini dell'adempimento degli obblighi imposti dal RGPD. Più precisamente il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta** (con il supporto dell'Amministratore di sistema, ove presente) dovranno **accertare che i dati oggetto di violazione siano dati personali nonché la probabilità o meno che l'evento abbia comportato dei rischi per i diritti e la libertà delle persone e la gravità del rischio così identificato**. Nello specifico verrà effettuato:

a) il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità) o altro evento;
b) l'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
c) l'identificazione degli interessati;
d) il contenimento del danno;

Tutte le operazioni effettuate devono essere tracciate e documentate.

3.2.1. valutazione dell'impatto sugli interessati

Considerando 75 del RGPD:
"*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di 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; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.*"
Considerando 76 del RGPD:
"*La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una*

valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato."

Nella fase di valutazione, sulla base delle informazioni rinvenute, occorre innanzitutto stabilire se nell'incidente sono coinvolti i **dati personali**. In caso di risposta positiva occorre valutare l'impatto sugli interessati:

a) ove si tratta di una *violazione di riservatezza* occorre verificare che le misure di sicurezza (es.: cifratura dei dati) in uso rendano improbabile l'identificazione degli Interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note);
b) in caso di *perdita di integrità o disponibilità* di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli Interessati.

Si noti che **la valutazione del rischio per i diritti e le libertà delle persone, a seguito di una violazione, ha un focus diverso rispetto al rischio considerato nell'ambito di una Valutazione d'impatto sulla Protezione dei Dati Personali (c.d. DPIA)**.

La DPIA considera sia i rischi derivanti dal trattamento dei dati effettuato come previsto, sia i rischi in caso di violazione. Quando si valuta una potenziale violazione, si considera in termini generali la probabilità che questa si verifichi ed il danno che potrebbe derivarne all'Interessato; in altre parole, si tratta di una valutazione di un evento ipotetico.

Nel caso di una violazione effettiva, l'evento si è già verificato e, quindi, l'attenzione deve concentrarsi tutta sul rischio derivante dall'impatto della violazione sui singoli individui.

I fattori da considerare nella valutazione del rischio per i diritti e le libertà delle persone fisiche interessate dalla violazione possono così essere esemplificati (trattasi di elencazione non esaustiva né vincolante):

FATTORE	OSSERVAZIONI
Aspetti **generali**	Valutazione della gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche e della probabilità che tale impatto si verifichi. Se le conseguenze di una violazione sono più gravi, il rischio è più elevato; analogamente, se la probabilità che tali conseguenze si verifichino è maggiore, maggiore sarà anche il rischio
Tipo di **violazione**	Distruzione, modifica, perdita, divulgazione (ad esempio, una violazione della riservatezza può avere conseguenze diverse rispetto ad una violazione in cui i dati siano stati persi e non più disponibili)
Natura, carattere sensibile e volume dei **dati** personali	Alcuni tipi di dati personali possono sembrare relativamente innocui, tuttavia occorre valutare attentamente ciò che questi dati possono rivelare sull'Interessato a malintenzionati. Quando la violazione riguarda categorie particolari di dati personali (art. 9 del RGPD) e dati relativi a condanne penale e reati (art. 10 del RGPD), il rischio per i diritti e le libertà degli Interessati dovrebbe essere, sempre, considerato presente.

	Inoltre, di norma, una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale. Una violazione che interessi grandi quantità di dati personali relative a molte persone può avere ripercussioni su un numero corrispondentemente elevato di persone.
Facilità di **identificazione** delle persone fisiche	Facilità di identificazione, diretta o indiretta tramite abbinamento con altre informazioni, di specifiche persone fisiche sulla base dei dati personali compromessi dalla violazione. L'identificazione può essere direttamente o indirettamente possibile a partire dai dati oggetto di violazione; tuttavia, può dipendere anche dal contesto specifico della violazione e dalla disponibilità pubblica dei corrispondenti dettagli personali. Ciò potrebbe essere più rilevante per le violazioni della riservatezza e della disponibilità. Sebbene i dati personali protetti da un adeguato livello di crittografia siano incomprensibili a persone non autorizzate, senza la chiave di decrittazione, le sole tecniche di pseudonimizzazione non possono essere considerate tali da rendere i dati incomprensibili.

FATTORE	OSSERVAZIONI
Gravità delle **conseguenze** per le persone fisiche	Danno potenziale alle persone fisiche che potrebbe derivare dalla violazione, comprese le categorie degli interessati e dei dati personali coinvolti e la permanenza a lungo termine delle conseguenze del danno (furto di identità, danni fisici, disagio psicologico, danni reputazionali). A seconda della natura dei dati personali coinvolti in una violazione (ad esempio, categorie particolari di dati), il potenziale danno che potrebbe derivare alle persone può essere particolarmente grave, in particolare laddove la violazione possa comportare il furto o frode di identità, danni fisici, disagio psicologico, umiliazione o danno alla reputazione. Il fatto che si sappia o meno che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale. Si dovrebbe altresì tener conto della permanenza delle conseguenze per le persone fisiche laddove l'impatto possa essere considerato maggiore qualora gli effetti siano a lungo termine.
Caratteristiche particolari del **Titolare**	La natura e il ruolo del Titolare del trattamento e delle sue attività possono influire sul livello di rischio per le persone fisiche in seguito a una violazione.

Caratteristiche particolari dell'**Interessato**	Se la violazione riguarda dati personali relativi a persone fisiche vulnerabili (minori, anziani, pazienti, …), queste ultime potrebbero essere esposte a un rischio maggiore di danni.
Numero di persone fisiche interessate	Di norma, maggiore è il numero di persone fisiche interessate, maggiore è l'impatto che una violazione può avere. Tuttavia, una violazione può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi.

Qualora il numero degli interessati (anche potenziali) dalla violazione sia ridotto e questi siano identificabili è opportuno stilare degli elenchi da utilizzare nel caso in cui il sia necessario inviare loro delle comunicazioni personalizzate.

3.2.2. valutazione della probabilità e gravità del rischio

La gravità di una violazione di dati personali è definita come la **stima dell'entità del potenziale impatto sulle persone fisiche derivante dalla violazione medesima**. Tale valutazione di impatto permette di stabilire la necessità di notifica della violazione all'Autorità di controllo, in particolare se sia probabile un rischio per la libertà e diritti delle persone fisiche, e la comunicazione anche agli Interessati, nel caso in cui tale rischio sia elevato.

La violazione dei dati può comportare **rischi per i diritti e le libertà delle persone** fisiche. I rischi principali sono connessi alla possibilità che l'Interessato subisca danni fisici, materiali o immateriali connessi perdita del controllo dei dati personali quali, ad esempio:

a) limitazione dei diritti;
b) discriminazione;
c) furto o usurpazione di identità;
d) perdite finanziarie;
e) decifratura non autorizzata della pseudonimizzazione;
f) pregiudizio alla reputazione;
g) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari);
h) qualsiasi altro danno economico o sociale, significativo.

La **tabella** che segue rappresenta visivamente i livelli di gravità del rischio "*per i diritti e le libertà delle persone fisiche*" coinvolte:

	Impatto della violazione sui diritti e le libertà delle persone coinvolte
GRAVITÀ	**BASSO**: gli individui possono andare incontro a *disagi minori*, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.);
	MEDIO: gli individui possono andare incontro a *significativi disagi*, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.);
	ALTO: gli individui possono andare incontro a *conseguenze significative*, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni

	alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.);
	MOLTO ALTO: gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.)

Nel valutare il livello complessivo di rischio che potrebbe derivare da una violazione, il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta** devono considerare una combinazione tra la gravità del potenziale impatto sui diritti e sulle libertà delle persone e la probabilità che esso si verifichi.

Con specifico riferimento alla violazione di dati personali, il livello di probabilità è ritenuto rilevante secondo il seguente schema:

PROBABILITÀ	**Possibilità che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**
	IMPROBABILE
	PROBABILE

Le Linee Guida suggeriscono di ritenere, il rischio elevato per i diritti e le libertà delle persone fisiche, quantomeno come "probabile" quando la violazione riguardi dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oppure che includono 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.

RIASSUMENDO

	Descrizione	Notifica all'Autorità	Comunicazione agli interessati
Rischio	**BASSO**: nessun pregiudizio sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	NO	NO
	MEDIO: probabile pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	NO
	ALTO e MOLTO 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, acquisito un ragionevole grado di certezza del fatto che sia avvenuto un incidente per la sicurezza delle informazioni che abbia compromesso dati personali, il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta**:

a) stimano la gravità e la probabilità della violazione e classifica il rischio;
b) documentano la decisione presa a seguito della valutazione del rischio nel Registro delle violazioni.

Gli elementi a supporto del procedimento e degli esiti della valutazione del rischio sono documentati utilizzando il modello **ALLEGATO D – "Modulo di valutazione del**

rischio connesso al violazione di dati personali" e tale documentazione è conservata in apposito archivio.

SCENARI AL TERMINE DELLA FASE VALUTATIVA

A) ove i **rischi per gli interessati siano trascurabili**, la procedura può terminare, dopo aver documentato il processo e le scelte operate: le misure messe in atto sono state adeguate alla minaccia. Una eventuale fase di miglioramento può essere innescata per incrementare ulteriormente la protezione del dato, ma non è obbligatoria.

L'art. 33 paragrafo 1 chiarisce, infatti, che **non vi è obbligo di notifica della violazione quando è "*improbabile*" che questa comporti un rischio per i diritti e le libertà delle persone fisiche**. Tuttavia, si ricorda che, sebbene inizialmente la notifica possa non essere richiesta in quanto non esiste un rischio probabile per i diritti e le libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e **il rischio dovrebbe essere rivalutato**.

B) nel caso in cui i **rischi per l'Interessato non siano trascurabili** occorre procedere alla notificazione all'Autorità di controllo sulla scorta delle indicazioni di cui al successivo paragrafo 4. In questo caso, la procedura deve dare le giuste priorità agli sforzi di contenimento dell'incidente. In ogni caso, andrà condotta una successiva fase di miglioramento.

C) qualora i **rischi per l'Interessato siano elevati** occorre procedere alla comunicazione della violazione alle persone fisiche interessate, di cui al successivo paragrafo 6, in aggiunta alla notificazione all'Autorità di controllo, salvo che quest'ultima richieda di omettere o ritardare la comunicazione stessa. In ogni caso, andrà condotta una fase di miglioramento.

3.3. Tool di autovalutazione del Garante privacy

Il Garante per la Protezione dei Dati Personali ha reso disponibile uno specifico Tool che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

Mediante alcuni semplici quesiti, il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta** vengono guidati nell'assolvimento degli obblighi in materia di «Notifica di una violazione dei dati personali all'autorità di controllo» (art. 33 del RGPD) e di «Comunicazione di una violazione dei dati personali all'interessato» (art. 34 del RGPD). Tale strumento è da considerarsi esclusivamente quale ausilio al processo decisionale del Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta e non rappresenta un pronunciamento del Garante sulle informazioni fornite e sulle valutazioni effettuate. Le informazioni fornite durante il suo utilizzo non saranno conservate.

LINK al **sito web**: https://servizi.gpdp.it/databreach/s/self-assessment

3.4. Valutazioni supplementari

Ulteriori analisi dell'accaduto possono rendersi necessarie qualora:

a) il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta** ritengano necessario un approfondimento finalizzato ad es. all'integrazione di una precedente notifica all'Autorità di controllo;

b) l'Autorità di controllo, gli organi di polizia o la magistratura ritengano necessarie informazioni aggiuntive od approfondimenti di informazioni già fornite;
c) durante una delle fasi del processo di gestione del data breach siano emerse situazioni non approfondibili o non sia stato possibile coinvolgere pienamente responsabili esterni o questi non abbiano comunicato in tempo utile i risultati delle loro analisi.

L'analisi supplementare può essere attivata più volte per la stessa violazione, secondo necessità.

4. Notifica della violazione dei dati personali all'Autorità di controllo

Considerando 88 del RGPD:
"*Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.*"

4.1. Quando effettuare la notificazione

Art. 33, par. 1, del RGPD
"*In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, 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*"

Considerando 87 del RGPD:
"*È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento.*"

La normativa prevede che, **non appena si venga a conoscenza di una violazione dei dati personali che presenti un rischio per i diritti e le libertà delle persone coinvolte**, sia obbligatorio effettuare la notifica all'Autorità. Pertanto, **la notifica all'Autorità dell'avvenuta violazione non è un processo automatico, essendo subordinata alla valutazione del rischio per gli interessati che spetta al Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta**.

Le Linee guida chiariscono quando il Titolare del trattamento possa considerarsi "*a conoscenza*" di una violazione.

L'EDPB ritiene che il Titolare del trattamento debba considerarsi "*a conoscenza*" nel momento in cui sia ragionevolmente certo che si è verificato un incidente di sicurezza che abbia portato alla compromissione dei dati personali. Tuttavia, va considerato che il RGPD impone al Titolare del trattamento di attuare tutte le misure tecniche ed organizzative di protezione adeguate a stabilire, immediatamente, se si sia verificata una violazione ed informare tempestivamente l'Autorità di controllo e gli interessati. L'EDPB afferma, inoltre, che è opportuno stabilire il fatto che la notifica sia stata

trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione e delle sue conseguenze e dei suoi effetti negativi per l'Interessato.

Il Titolare del trattamento è quindi tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva, in modo da poter adottare le misure appropriate.

Il momento esatto in cui il Titolare del trattamento possa considerarsi "*a conoscenza*" di una particolare violazione dipenderà dalle circostanze della violazione.

Nella pratica, rilevazione e valutazione dell'evento sono spesso interconnesse e già nell'immediato può essere riscontrato un rischio ragionevole di violazione e, anche se non sono disponibili subito maggiori informazioni di dettaglio, si rende necessaria una preventiva notificazione all'Autorità di controllo. Vi sono casi, tuttavia, in cui è possibile definire se l'evento costituisca una violazione ai sensi del RGPD solo al termine della fase di valutazione. Acquisita la notizia di un possibile data breach il Titolare del trattamento può aver necessità di un breve periodo nel quale effettuare indagini, proprio al fine di stabilire se si sia verificata, o meno, una violazione. Durante questo periodo di indagine il Titolare del trattamento non può essere considerato "consapevole".

Le Linee Guida prevedono, tuttavia, che l'indagine iniziale venga avviata quanto prima e stabilisca con un ragionevole grado di certezza se si sia verificata una violazione; potrà poi seguire un'indagine più approfondita. In questo caso la decorrenza della tempistica per la notificazione all'Autorità di controllo è, comunque, dal momento della constatazione.

Qualora i contorni della violazione non siano chiari si può attendere fino ad **un massimo di 72 ore** prima di effettuare una notifica (Non si tratta di un termine puramente indicativo ma **categorico**, il cui mancato rispetto se non adeguatamente motivato, integra una situazione sanzionabile). Alla scadenza delle 72 ore è comunque necessario fare una comunicazione, significando che questa è l'inizio di una notifica in fasi. Il RGPD consente infatti una notifica per fasi, a condizione che il Titolare indichi i motivi del ritardo, in conformità all'art. 33, paragrafo 1.

In ogni caso, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, essa va corredata dei **motivi del ritardo**. Si suggerisce in ogni caso di procedere comunque all'effettuazione della notifica entro il termine, fatto salvo quanto *infra* con riferimento alla notifica per fasi.

L'obiettivo dell'obbligo di notifica è incoraggiare i Titolari del trattamento ad agire tempestivamente in caso di violazione, a contenerla e, se possibile, a recuperare i dati personali compromessi, nonché a chiedere il parere pertinente all'Autorità di controllo. La notifica all'Autorità di controllo entro le prime 72 ore può, inoltre, consentire al Titolare del trattamento di assicurarsi che le decisioni in merito alla comunicazione od alla mancata comunicazione all'Interessato siano corrette.

Si ricorda che **l'obbligo di effettuare la notifica all'Autorità di controllo, ricorre solo quando:**

a) l'Ente è Titolare del trattamento di dati coinvolti nell'incidente;
b) l'Ente è Contitolare del trattamento e l'accordo di contitolarità prevede che spetti ad esso procedere alla notifica, anche per conto dell'altro Contitolare;
c) l'Ente è Responsabile del trattamento con delega alla notifica. L'Ente non ha il dovere di notificare la violazione all'Autorità di controllo quando agisce come Responsabile del trattamento per conto di altro Titolare, senza delega alla notifica. In questo caso l'Ente deve comunicare al Titolare del trattamento la sospetta violazione e/o l'incidente di sicurezza riguardante dati personali, nei modi convenuti, con la massima tempestività e mettersi a disposizione di quest'ultimo per approfondimenti e contenimento dei danni.

4.2. Come effettuare la notificazione

Per le violazioni identificate, il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta** provvedano alla notifica della violazione, **utilizzando gli strumenti ed in conformità alle istruzioni rese disponibili dall'Autorità di controllo**, **previa consultazione ed in collaborazione con il RPD**.

Alla data di redazione del presente documento il Garante della Protezione dei Dati Personali ha reso disponibile un **servizio di notificazione telematica**, raggiungibile al seguente indirizzo web:

https://servizi.gpdp.it/databreach/s/

Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante, ma utile per vedere in anteprima i contenuti che andranno comunicati all'Autorità.

Si ricorda che, per semplificare gli adempimenti previsti per i Titolari del trattamento, il Garante ha ideato e messo disposizione un apposito **strumento di autovalutazione (self assessment)** che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza. Lo strumento è presente all'interno della pagina web sopra indicata.

4.2.1. Informazioni da fornire

Art. 33, par. 3, del RGPD
"*La notifica di cui al paragrafo 1 deve almeno:*
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere 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."

L'art. sopra riportato stabilisce che il Titolare del trattamento debba "***almeno***" fornire queste informazioni all'Autorità di controllo mediante lo strumento della notifica, in modo che il Titolare possa, se necessario, scegliere di fornire ulteriori dettagli. Differenti tipi di violazioni (riservatezza, integrità o disponibilità) potrebbero richiedere di fornire ulteriori informazioni per spiegare puntualmente le circostanze di ciascuna fattispecie.

In ogni caso, l'Autorità di controllo potrà richiedere **ulteriori dettagli** nell'ambito della propria attività d'indagine.

Il RGPD non definisce le "*categorie di interessati*" o cosa si intenda per "*registrazioni di dati personali*".

Tuttavia, l'EDPB suggerisce, quanto alle categorie di interessati, di fare riferimento ai vari tipi di soggetti i cui dati personali siano stati colpiti da una violazione: a seconda dei descrittori utilizzati, ciò potrebbe includere, tra gli altri, bambini ed altri gruppi vulnerabili, persone con disabilità, dipendenti o fruitori di particolari servizi.

Allo stesso modo, in relazione alle categorie di registrazioni di dati personali, si potrebbe fare riferimento ai diversi tipi di record che il Titolare del trattamento si trovi a trattare, come dati sanitari, documenti scolastici, informazioni sull'assistenza sociale, informazioni relativi a provvedimenti dell'Autorità giudiziaria, dettagli finanziari, numeri di conto bancario, numeri di carta d'identità, passaporto e così via.

Il considerando 85 del RGPD chiarisce che uno degli scopi della notifica è limitare i danni alle persone. Di conseguenza, se le tipologie di Interessati o di dati personali implicano un rischio di danno particolare che si verifica a seguito di una violazione (ad esempio, furto di identità, frode, perdita finanziaria, minaccia al segreto professionale), ecc., allora è importante che la notifica indichi queste categorie. Ad esso si collega, in tal modo, l'obbligo di descrivere le probabili conseguenze della violazione.

Laddove non fossero disponibili informazioni precise (ad esempio, il numero esatto degli interessati o di registrazioni), ciò non dovrebbe costituire un ostacolo alla tempestiva notifica della violazione. L'EDPB consente di effettuare approssimazioni nel numero di persone interessate e nel numero di registrazioni di dati personali coinvolti. L'attenzione dovrebbe essere rivolta ad affrontare gli effetti negativi della violazione piuttosto che fornire cifre precise. Pertanto, quando fosse evidente che si è verificata una violazione, ma la sua portata non fosse ancora nota, la notifica in fasi (di cui al successivo paragrafo) sarebbe un modo sicuro per soddisfare gli obblighi di notifica.

4.2.2. Notifica "per fasi"

Art. 33, par. 4 del RGPD:
"*Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente,* ***le informazioni possono essere fornite in fasi successive*** *senza ulteriore ingiustificato ritardo*"

A seconda della natura della violazione, potrebbero essere necessarie ulteriori indagini da parte del **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta** (anche valendosi della collaborazione di eventuali Responsabili del trattamento) per stabilire tutti i fatti rilevanti relativi all'incidente.

È probabile che ciò avvenga nel caso di violazioni più complesse, come alcuni tipi di incidenti che coinvolgono la sicurezza informatica nei quali, ad esempio, potrebbe essere necessaria un'indagine forense approfondita per stabilire puntualmente la natura della violazione e la misura in cui i dati personali siano stati violati o compromessi. Di conseguenza, in questi casi il Titolare del trattamento dovrà svolgere ulteriori indagini e fornire ulteriori informazioni in un secondo momento.

Ciò è consentito, a condizione che il Titolare del trattamento giustifichi il ritardo, ai sensi dell'art. 33, paragrafo 1, del RGPD.

L'EDPB raccomanda che, quando il Titolare del trattamento notifica per la volta l'Autorità di controllo, esso possa precisare anche se non dispone ancora di tutte le informazioni richieste, impegnandosi a fornire maggiori dettagli in seguito. L'Autorità di controllo dovrebbe concordare su "come" e "quando" andrebbero fornite informazioni aggiuntive; ciò, tuttavia, non impedisce al Titolare del trattamento di fornire ulteriori informazioni in qualsiasi altra fase, qualora venga a conoscenza di ulteriori dettagli rilevanti sulla violazione che debbano essere forniti all'Autorità di controllo.

Dopo aver effettuato una notifica "iniziale", il Titolare del trattamento potrebbe, inoltre, informare l'Autorità di controllo del fatto che, a fronte di un'indagine successiva, siano emersi elementi tali da far ritenere che l'incidente di sicurezza fosse di minor impatto per l'Interessato o, anche, che non si fosse verificata alcuna violazione.

Non è prevista alcuna sanzione per la segnalazione di un incidente che, a seguito di indagini più approfondite, non risultasse essere una violazione.

4.2.3. Notifiche "ritardate" e "cumulative"

Art. 33, par. 1 del RGPD:
"(…) *Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei* ***motivi del ritardo***"

Detta previsione, unitamente alla possibilità di effettuare una notifica "per fasi", rende evidente il fatto che il Titolare del trattamento potrebbe non essere sempre in grado di notificare una violazione "*senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza*" e che, pertanto, una notifica tardiva sia da considerarsi ammissibile.

L'EDPB segnala che uno scenario di questo tipo potrebbe verificarsi laddove, ad esempio, il Titolare del trattamento subisse molteplici violazioni simili, in un breve periodo di tempo, che colpissero allo stesso modo un gran numero di Interessati. Il Titolare potrebbe, in tal caso, venire a conoscenza di una violazione e, avviando l'indagine e prima della notifica, individuare ulteriori violazioni simili, dovute a cause diverse. A seconda delle circostanze, il Titolare del trattamento potrebbe impiegare del tempo per stabilire l'entità delle violazioni e, invece di notificare ciascuna violazione individualmente, potrebbe decidere di procedere con una notifica unitaria che rappresentasse le diverse violazioni. Ciò, potrebbe comportare un ritardo nella notifica all'Autorità di controllo.

Sebbene ogni singola violazione costituisca un incidente da segnalare, per evitare di essere eccessivamente formalista, l'EDPB ammette che il Titolare del trattamento possa procedere ad una notifica "cumulativa" che rappresenti tutte queste violazioni, a condizione che riguardi lo stesso tipo di dati personali, violati nello stesso modo, in un arco di tempo relativamente breve.

Laddove, invece, si trattasse di una serie di violazioni che riguardasse diversi tipi di dati personali, violati in modi diversi, la notifica dovrebbe procedere normalmente, segnalando ciascuna violazione in conformità a quanto previsto dall'art. 33 del RGPD.

Sebbene la normativa consenta, in una certa misura, notifiche tardive, ciò non dev'essere visto come qualcosa che possa avvenire nell'ordinario.

Vale la pena di precisare che è sempre possibile inviare notifiche "cumulative", inerenti più violazioni simili "*senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza*".

4.3. Condizioni per le quali non è richiesta la notifica

Art. 33, par. 1, del RGPD:
"*In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza,* ***a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche***."

Un esempio potrebbe essere il caso in cui i dati personali fossero già disponibili al pubblico e la divulgazione di tali dati non costituisse un probabile rischio per l'individuo.

Nel parere 03/2014 sulla notifica delle violazioni, il WP29 ha spiegato che una violazione della riservatezza dei dati personali crittografati con un algoritmo all'avanguardia costituisca pur sempre una violazione dei dati personali e debba essere notificata. Tuttavia, ove la riservatezza della chiave fosse intatta (cioè, la chiave non fosse stata compromessa in alcuna violazione della sicurezza e fosse stata generata in modo tale da non poter essere scoperta con i mezzi tecnici disponibili da qualsiasi persona non autorizzata ad accedervi) allora i dati potrebbero essere, in linea di principio, considerati incomprensibili. Pertanto, sarebbe improbabile che la violazione potesse incidere negativamente sugli individui e, ciò, renderebbe non necessaria la notifica.

Ciò nonostante, anche quando i dati fossero crittografati, una perdita od un'alterazione potrebbe avere conseguenze negative per gli Interessati qualora il Titolare del trattamento non disponesse di backup adeguati (perdita di disponibilità).

A conclusioni analoghe il WP29 è pervenuto in relazione alla fattispecie in cui dati personali, come le password, fossero sottoposti ad "hashing" con "salt", il valore di hash fosse calcolato con una funzione hash con chiave crittografica all'avanguardia, la chiave utilizzata per eseguire l'hashing dei dati non fosse compromesse in alcuna violazione e la chiave utilizzata per eseguire l'hashing dei dati fosse stata generata in modo tale da non poter essere accertata con i mezzi tecnologici disponibili da alcuna persona non autorizzata ad accedervi.

Secondo l'EDPB, ove i dati personali fossero stati resi sostanzialmente incomprensibili a soggetti non autorizzati ed ove dei dati medesimi esistesse una copia od un backup, potrebbe non essere necessario notificare all'Autorità di controllo la violazione della riservatezza. Questo in quanto sarebbe improbabile che una tale violazione possa rappresentare un rischio i diritti e le libertà degli individui.

Tuttavia, va tenuto presente che, sebbene inizialmente la notifica potrebbe non essere richiesta (non essendo probabile un rischio per i diritti e le libertà degli individui), ciò potrebbe cambiare nel tempo ed il rischio dovrebbe essere rivalutato (ad esempio, se, successivamente, si scopre che la chiave fosse stata compromessa o venisse scoperta una vulnerabilità nel software di crittografia) e potrebbe rendersi, comunque, necessaria una notifica.

Inoltre, va notato che laddove si verificasse una violazione in cui non esistessero backup dei dati personali crittografati, allora si sarebbe in presenza di una violazione della

disponibilità, che potrebbe comportare rischi per le persone e, pertanto, potrebbe rendersi necessaria una notifica.

Allo stesso modo, laddove si verificasse una violazione che comportasse la perdita di dati crittografati, anche in presenza di un backup dei dati personali, ciò potrebbe comunque costituire una violazione da notificare, a seconda del tempo impiegato per ripristinare i dati da tale backup e dell'effetto che la mancanza di disponibilità avrebbe sugli Interessati.

4.4. Eventuali ulteriori notificazioni all'Autorità di controllo

Effettuata la notifica in favore dell'Autorità di controllo, è poi opportuno verificare se sia necessaria una *seconda notifica*, più approfondita, quale conseguenza di un'analisi tecnica supplementare ovvero di elementi ed informazioni successivamente acquisiti.

È opportuno inoltre precisare che se, dopo la notifica iniziale, una successiva indagine dimostrasse che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione, il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta** dovrebbero informarne l'Autorità di controllo. Tali informazioni possono quindi essere aggiunte alle informazioni già fornite all'Autorità di controllo e l'incidente può essere quindi registrato come un evento che non costituisce una violazione.

Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione.

5. Recepimento della eventuale risposta dell'Autorità di controllo

Il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta** dispongono con sollecitudine ulteriori indagini o eventuali misure correttive, secondo le disposizioni ricevute dall'Autorità di controllo. Parimenti, provvede a seguito del ricevimento di indicazioni od ordini relativamente alla comunicazione da effettuare o non effettuare in favore degli interessati.

6. Comunicazione della violazione dei dati personali all'Interessato

Art. 34, par. 1, del RGPD:

"*Quando la violazione dei dati personali è* ***suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche****, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo*"

Considerando 86 del RGPD:

"*Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di*

dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione."

Contestualmente alla decisione di notificare all'Autorità di controllo, occorre valutare se sia il caso di informare anche gli Interessati. Il modello di notificazione predisposto dall'Autorità di controllo richiede infatti una specifica indicazione e descrizione delle circostanze e valutazioni che abbiano condotto ad effettuare o non effettuare siffatta comunicazione agli interessati.

La soglia di rischio determinante per rendere necessaria la comunicazione di una violazione ai singoli Interessati è più elevata rispetto a quella utilizzata come indicatore della necessità della notifica all'Autorità di controllo e, pertanto, non tutte le violazioni dovranno essere comunicate all'Interessato. **A tale scopo va valutata la gravità del rischio per gli interessati ed i loro diritti**.

Nel caso di accertamento di una **violazione di 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 precedente paragrafo 3, il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta**, provvederanno ad informare gli Interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio. In tale ipotesi occorre quindi valutare:

a) la fattibilità di contattarli singolarmente oppure la necessità di procedere con pubblicazioni su diversi mezzi di comunicazione (sito web, quotidiani, radio, tv);
b) le misure di contenimento che gli stessi interessati possano mettere in atto per minimizzare i rischi;
c) le forme di comunicazione più comprensibili per gli interessati (mezzi, lingue, linguaggio) come indicato nelle Linee guida elaborate dal Gruppo ex art. 29 in materia di trasparenza (WP 260), aggiornate in base alle previsioni del Regolamento (UE) 2016/679.

Anche di questa fase deve essere prodotta e conservata appropriata documentazione.

6.1. Quando effettuare la comunicazione

Art. 34, par. 1, del RGPD:
"*Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato* ***senza ingiustificato ritardo.***"

Il RGPD afferma che la comunicazione di una violazione agli interessati dovrebbe avvenire "***senza ingiustificato ritardo***", il che significa il prima possibile. **L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi**. A seconda della natura della violazione e del rischio presentato, la comunicazione tempestiva aiuterà le persone a prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

Da notare inoltre che il Considerando 86 suggerisce che "T*ali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge*". Parallelamente, il Considerando 88 indica che la notifica di una violazione dovrebbe tenere "*conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali*".

Conseguentemente si ritiene suggeribile, **nel contesto della notifica all'Autorità di controllo, formulare espressa richiesta di indicazioni in tal senso** (non soltanto se provvedere alla comunicazione o no, ma anche quale contenuto della comunicazione e quali canali suggeriti).

Le Linee Guida emanate dall'EDPB, suggeriscono le seguenti fattispecie, quali indicatori del fatto che la violazione possa comportare un "*rischio elevato per i diritti e le libertà delle persone fisiche*":

- attacco informatico ad un servizio online, con esfiltrazione dei dati personali ivi presenti (anche se riguardanti le credenziali di accesso e/o la cronologia e/o i log);
- attacco mediante ransomware agli archivi del Titolare del trattamento, in assenza di backup o, comunque, in caso di impossibilità di ripristino;
- i dati personali di un interessato sono stati erroneamente comunicati ad altro Interessato;
- comunicazioni e-mail a destinatari errati;
- indisponibilità di dati e/o documenti protratta per un periodo di tempo significativo;

6.2. Come effettuare la comunicazione

Considerando 86 del RGPD:
"(…) *Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e* ***in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti*** *quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione*"

Per la comunicazione, è possibile identificare **uno o più canali di comunicazione**, a seconda delle circostanze, quali comunicazioni e-mail, comunicazioni PEC, SMS, posta ordinaria, comunicati istituzionali, banner o notifiche su siti web, scegliendo il canale che massimizza la probabilità che tutti gli interessati siano raggiunti dal messaggio.

Di regola, la violazione dovrebbe essere comunicata direttamente a ciascun Interessato, a meno che ciò comporti uno sforzo sproporzionato. In tal caso, è tuttavia prevista una comunicazione pubblica od un provvedimento analogo, con il quale gli interessati vengano informati in modo altrettanto efficace (art. 34, paragrafo 3, lettera c), del RGPD).

Caso per caso, il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta**, dovranno **sempre privilegiare la modalità di comunicazione diretta** con i soggetti interessati (quali e- mail, PEC, SMS o messaggi diretti) eventualmente anche combinando modalità differenti. Inoltre, nel contesto della notificazione all'Autorità di controllo, potranno essere richiesti suggerimenti in ordine ai tempi, alla modalità preferibile ed al contenuto della comunicazione agli Interessati.

Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori.

Non dovrà essere utilizzato il canale di contatto compromesso dalla violazione, in quanto tale canale potrebbe essere utilizzato anche da autori di attacchi che si presentino come questo Ente.

Ove non si abbia la possibilità di comunicare una violazione all'Interessato perché non si disponga di dati sufficienti per contattarlo, questi sarà informato non appena sia ragionevolmente possibile farlo (ad esempio quando l'Interessato esercita il proprio diritto. ai sensi dell'art. 15 del RGPD, di accedere ai dati personali e fornisce le informazioni necessarie per essere contattato).

6.3. Quali informazioni comunicare

Art. 34, par. 2, del RGPD:
"*La comunicazione all'interessato di cui al paragrafo 1 del presente art. descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e* ***contiene almeno le informazioni e le misure di cui all'art. 33, paragrafo 3, lettere b), c) e d).***"

Sebbene sia preferibile utilizzare il modello **ALLEGATO E – "Comunicazione all'Interessato della violazione dei dati personali"**, la comunicazione in altra forma deve comunque contenere, ai sensi dell'art. 34, le seguenti **informazioni**:

1) il nome ed i dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni;
2) una descrizione della natura della violazione;
3) una descrizione delle probabili conseguenze della violazione dei dati personali;
4) una descrizione delle 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;
5) se l'Autorità di controllo abbia suggerito od ordinato misure di gestione della violazione e sull'attenuazione del suo impatto;
6) eventuali indicazioni al destinatario sul modo in cui proteggersi dalle possibili conseguenze negative della violazione

Particolare attenzione dev'essere prestata con riferimento alle "*eventuali indicazioni al destinatario sul modo in cui proteggersi dalle possibili conseguenze negative della violazione*".

6.4. Quando non effettuare la comunicazione

Art. 34, parr. 3 e 4, del RGPD:
"3. ***Non è richiesta la comunicazione all'interessato*** *di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:*
a) 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;
b) 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 di cui al paragrafo 1;
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.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, ***l'autorità di controllo può richiedere****, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi* ***provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.***"

Il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta**, i quali ritengano di non procedere con la comunicazione agli Interessati, dovranno essere in grado di dimostrare all'Autorità di controllo la ricorrenza di una o più delle condizioni di cui all'art. 34, par. 3 del RGPD.

Si consideri, peraltro che, sebbene inizialmente la notifica possa essere ritenuta come non necessaria per assenza di rischio per i diritti e libertà delle persone fisiche, ciò potrebbe cambiare nel tempo a seguito del sopravvenire di ulteriori elementi informativi: in tal caso, il rischio dovrà essere rivalutato.

7. Altre segnalazioni

Il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta** dovranno verificare la necessità di informare altri organi quali, a mero titolo esemplificativo:
- CSIRT Italia (https://www.csirt.gov.it/segnalazione);
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti);
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche).
- Gestore di Identità Digitale ed AgID nel caso in cui si individui un uso anomalo di un'identità SPID, CIE, CNS, ecc.

Ciascuna segnalazione dovrà avvenire nel rispetto delle procedure ed utilizzando la modulistica all'uopo eventualmente predisposta da ciascuna Autorità di vigilanza o controllo.

8. Documentazione della violazione

Art. 33, par. 5, del RGPD:
"*Il titolare del trattamento* ***documenta qualsiasi violazione*** *dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo*"

La necessità di documentare le violazioni di dati personali è attuativa del principio di "accountability" (c.d. responsabilizzazione), contenuto nell'art. 5, paragrafo 2, del RGPD. Lo scopo della registrazione delle violazioni non notificabili, nonché delle violazioni notificabili, si riferisce anche agli obblighi del Titolare del trattamento previsti dall'art. 24 del RGPD e l'Autorità di controllo può richiedere di vedere tali registrazioni.

Si ricorda che **la mancata corretta documentazione di una violazione può comportare l'esercizio da parte dell'Autorità di controllo dei suoi poteri ai sensi dell'art. 58 del RGPD e l'imposizione di una sanzione amministrativa pecuniaria ai sensi dell'art. 83 del RGPD**.

Il Titolare del trattamento stabilisce di documentare gli incidenti di sicurezza e le violazioni di dati personali come segue:
a) adozione, di un registro "interno" delle (sole) violazioni di dati personali, intendendosi per tale un inventario aggiornato delle violazioni contenente tutte le informazioni necessarie a chiarire le circostanze nelle quali si sono verificate, le conseguenze che le stesse hanno avuto ed i provvedimenti adottati per porvi rimedio. Esso tiene traccia anche delle varie fasi di gestione dell'evento, dalla rilevazione, all'analisi e alla sua risoluzione e conclusione;
b) adozione di modulistica, anche a rilevanza esterna, idonea a documentare gli incidenti di sicurezza e le violazioni di dati personali.

Il RGPD non specifica un **periodo di conservazione** per tale documentazione. Essa sarà dunque conservata nel rispetto dei termini e delle norme di legge sulla conservazione della documentazione amministrativa, anche in considerazione del fatto che la conservazione è necessaria, in conformità dell'art. 33, paragrafo 5, nella misura in cui il Titolare del trattamento potrà essere chiamato a fornire prove all'Autorità di controllo in merito al rispetto di tale art. oppure, più in generale, del principio di responsabilizzazione.

8.1. il Registro delle violazioni

Il Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta sono responsabili della tenuta e dell'aggiornamento del Registro delle violazioni, sulla scorta delle informazioni e della documentazione acquisita.

Poiché il RGPD non specifica quale debba essere il **contenuto** e la **forma** del Registro delle violazioni né il tipo di supporto sul quale debba essere redatto, per estensione delle disposizioni contenute nell'art. n. 30 del RGPD (relativamente al registro delle attività di trattamento e registro delle categorie di attività di trattamento) si presume che tale registro possa anche essere **di tipo elettronico**. Il Titolare del trattamento ha quindi deciso di adottarlo in tale forma.

Il registro dovrà essere accompagnato da idonee misure di sicurezza atte a garantire **l'integrità e l'immodificabilità dei dati in esso registrati** quali ad esempio la protocollazione, la stampa, …). I dati presenti nel registro sono trattati nel rispetto del **principio di minimizzazione** e secondo le misure necessarie per mitigare i rischi di violazione dei dati personali.

Ogni segnalazione, comprese quelle **non veritiere**, deve essere soggetta a registrazione nel registro delle violazioni. Per ogni violazione di cui sia accertata l'esistenza, anche se non notificata all'Autorità di controllo e non comunicata agli interessati, **il registro ripoterà (almeno)**:

(con riferimento alla segnalazione)
- numerazione progressiva;
- data ed ora della segnalazione;
- dati identificative del segnalante;
- unità organizzativa coinvolta;
- organi informati;
- valutazione circa la rilevanza (o meno) della segnalazione quale violazione di dati personali;

(con riferimento alla violazione)
- luogo violazione;
- modalità della violazione;
- descrizione dei sistemi, apparati, reti, banche dati oggetto di data breach;
- la natura della violazione dei dati personali;
- altri elementi utili alla descrizione della violazione;

(con riferimento agli interessati)
- indicazione delle categorie di interessati coinvolti;
- indicazione del numero approssimativo di interessati coinvolti;

(con riferimento ai dati personali coinvolti)
- indicazione delle categorie dei dati personali coinvolte;
- indicazione del numero approssimativo di dati personali coinvolti;

(con riferimento alle conseguenze)

- descrizione delle previste (o verificate) conseguenze;
(con riferimento ai rimedi)
- indicazione delle misure adottate per porre rimedio alla violazione;
- indicazione delle misure proposte per porre rimedio alla violazione;
(con riferimento all'attenuazione delle conseguenze)
- indicazione delle misure adottate per attenuare i possibili effetti negativi;
- indicazione delle misure proposte per attenuare i possibili effetti negativi;
(con riferimento ai tempi di ripristino)
- indicazione della tempistica stimata
(con riferimento alla notifica all'Autorità di controllo)
- valutazione circa la probabilità (o improbabilità) che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche;
- effettuazione o meno della notificazione;
- ragioni della omessa notificazione all'Autorità di controllo;
- ragioni della tardiva notificazione all'Autorità di controllo;
(con riferimento alla comunicazione agli interessati)
- valutazione circa la possibilità che la violazione sia (o meno) suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- effettuazione o meno della comunicazione;
- ragioni della omessa comunicazione agli interessati.

8.2. Altri documenti ed informazioni

Ad integrazione di quanto riportato nel registro, il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta** raccolgono e **conservano tutti i documenti relativi ad ogni violazione**, compresi quelli inerenti alle circostanze ad essa relative, le sue conseguenze ed i provvedimenti adottati per porvi rimedio.

9. Fase di miglioramento

Una volta contenuti i rischi o le conseguenze della violazione ed adempiuto agli obblighi di notificazione e comunicazione previsti dal RGPD occorre dedicare attenzione alla fase di miglioramento delle misure tecniche ed organizzative in uso presso il Titolare del trattamento, al fine di evitare il ripetersi di incidenti analoghi.

Le azioni previste in questa fase sono:
- l'analisi della relazione dettagliata sull'incidente;
- la reiterazione del processo di Gestione del rischio;
- l'eventuale revisione di questo documento (se necessario) e di eventuali altri documenti collegati (es. analisi del rischio, misure di sicurezza, modulistica, ecc.);
- l'individuazione di controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
- la revisione del sistema di gestione della protezione dei dati;
- la revisione con cadenza almeno annuale della procedura descritta nel presente documento.

10. Fattispecie di contitolarità e responsabilità del trattamento

10.1. Contitolari del trattamento

Art. 26 del RGPD
"*1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare*

riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.
2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
(…)"

Sulla scorta della previsione sopra riportata, laddove il Titolare del trattamento si trovasse ad operare, unitamente ad altri soggetti, in fattispecie classificabili in termini di **contitolarità del trattamento** dei dati personali, il relativo accordo o convenzione dovrà contenere espressa determinazione di chi assumerà il comando o sarà responsabile del rispetto degli obblighi di cui agli articoli 33 e 34 del medesimo RGPD.

Si riporta, a titolo esemplificativo, una bozza di clausola:
"*1. In eventuali casi di violazione della sicurezza dei dati personali che comportino, accidentalmente od in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati e tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati nel contesto del progetto comune, l'attività di coordinamento ai fini dell'adempimento degli obblighi di cui agli articoli 33 e 34 del RGPD è affidata a _____ il quale curerà la predisposizione di un apposito documento (data breach policy), ove non già esistente ed adottato.*
2. Al verificarsi di una violazione di dati personali, il Contitolare non assegnatario dell'attività di coordinamento provvederà:
a) ad informare l'altro Contitolare tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione, fornendogli tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sugli Interessati coinvolti e le misure adottate per mitigare i rischi;
b) fornire assistenza per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Esso, inoltre, si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive ed attuando tutte le azioni correttive approvate e/o richieste dal Contitolare assegnatario dell'attività di coordinamento. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al Trattamento eseguito.
3. Ciascun Contitolare si impegna a predisporre e tenere aggiornato un registro interno delle violazioni di dati personali nonché a raccogliere e conservare 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."

10.1. Responsabili del trattamento

Art. 28, par. 3 del RGPD
"*I trattamenti da parte di un responsabile del trattamento sono disciplinati 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. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:
(…)
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
(…)"

Sulla scorta della previsione di cui sopra, laddove il Titolare del trattamento necessiti che il trattamento di dati personali venga effettuato per suo conto ad opera di altri soggetti qualificabili come **responsabili del trattamento**, il contratto od altro atto giuridico che vincoli tale soggetto al Titolare del trattamento dovrà contenere espressa previsione che il responsabile assista il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del RGPD, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

È opportuno notare che il Responsabile del trattamento non è tenuto a valutare preventivamente la probabilità del rischio derivante da una violazione prima di avvisare il Titolare del trattamento in quanto solo quest'ultimo deve effettuare tale valutazione nel momento in cui viene a conoscenza della violazione. Il Responsabile deve solo stabilire se si sia verificata una violazione ed avvisare il Titolare del trattamento.

Il Titolare del trattamento si avvale del Responsabile del trattamento per il raggiungimento delle proprie finalità; pertanto, in linea di principio, il Titolare dovrebbe essere considerato "consapevole" una volta che il Responsabile lo abbia informato della violazione. L'obbligo del Responsabile di informare il proprio Titolare del trattamento consente a quest'ultimo di affrontare la violazione e di determinare se sia tenuto o meno ad informare l'Autorità di controllo e le persone interessate.

Il Titolare del trattamento potrebbe anche voler indagare sulla violazione, poiché il Responsabile del trattamento potrebbe non essere in grado di conoscere tutti i fatti rilevanti relativi alla questione, ad esempio, se sia ancora conservata una copia od un backup dei dati personali distrutti o persi dal Responsabile del trattamento. Ciò potrebbe influire sulla necessità o meno del Titolare del trattamento di effettuare la notifica.

Il RGPD non prevede un termine esplicito entro il quale il Responsabile del trattamento debba avvisare il Titolare, salvo che debba farlo "*senza ingiustificato ritardo*". Pertanto, l'EDPB raccomanda al Responsabile del trattamento di informare tempestivamente il Titolare, fornendo ulteriori informazioni sulla violazione man mano che maggiori dettagli diventino disponibili. Ciò, è importante per aiutare il Titolare del trattamento a soddisfare l'obbligo di notifica all'Autorità di controllo entro 72 ore.

Un Responsabile del trattamento potrebbe effettuare una notifica per conto del Titolare del trattamento di Genova, nel caso in cui quest'ultimo gli avesse concesso un'adeguata autorizzazione e, ciò, rientrasse negli accordi contrattuali tra Titolare e Responsabile. Tuttavia, è importante ricordare che la responsabilità legale di notificare rimarrebbe in capo al Titolare del trattamento.

Anche in questo caso, si riporta, a titolo esemplificativo, una bozza di clausola:
"*1. In eventuali casi di violazione della sicurezza dei dati personali che comportino, accidentalmente od in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati e tali da mettere a rischio i diritti e le libertà degli individui i cui dati*

personali sono trattati dal Responsabile per conto del Titolare (c.d. data breach), il Responsabile deve osservare le disposizioni organizzative contenute nella data breach policy adottata dal Titolare e, in ogni caso:
a) informare il Titolare tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione e fornire al Titolare tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sul Titolare e sugli Interessati coinvolti e le misure adottate per mitigare i rischi. Spetta unicamente al Titolare del trattamento di effettuare la valutazione circa la probabilità di rischio derivante dalla violazione stessa;
b) fornire assistenza al Titolare per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Il Responsabile si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive al Titolare ed attuando tutte le azioni correttive approvate e/o richieste dal Titolare. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al Trattamento eseguito;
2. I Responsabile del trattamento si impegna a predisporre e tenere aggiornato un registro interno delle violazioni di dati personali nonché a raccogliere e conservare 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."

ALLEGATI

ALLEGATO A – "DIAGRAMMA DI FLUSSO"

ALLEGATO B – "Modulo di segnalazione di una potenziale violazione di dati personali"

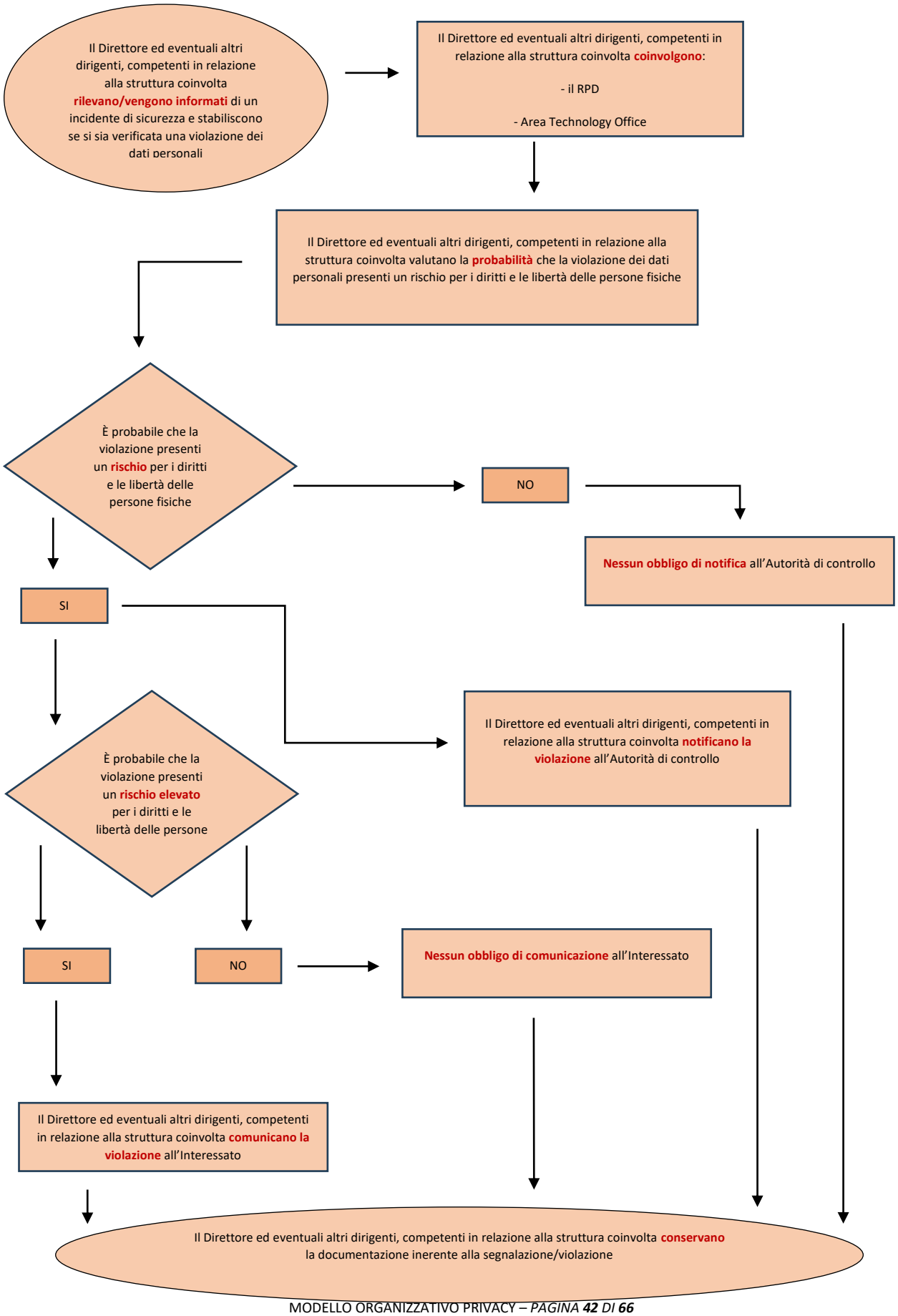
ALLEGATO C – "Modulo di inoltro di segnalazione di una potenziale violazione di dati personali"

ALLEGATO D – "Modulo di valutazione del rischio connesso al violazione di dati personali"

ALLEGATO E – "Comunicazione all'Interessato della violazione dei dati personali"

ALLEGATO F – "Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali"

ALLEGATO A - DIAGRAMMA DI FLUSSO



ALLEGATO B

MODULO DI SEGNALAZIONE DI UNA POTENZIALE VIOLAZIONE DI DATI PERSONALI

ai sensi dell'art. 33 del Regolamento Generale sulla Protezione dei Dati

(Il presente modello non è vincolante, ben potendo la segnalazione essere fornita in forma libera)

Il presente modulo va compilato da chiunque constati un effettivo o potenziale incidente di sicurezza che possa comportare una violazione di dati personali, al fine di consentire al Titolare del trattamento la valutazione e gestione dell'incidente stesso e, in caso di violazione accertata, di notifica al Garante e di comunicazione agli interessati.

Il modulo, compilato in ogni sua parte e debitamente sottoscritto, dev'essere consegnato al più presto con le seguenti alternative modalità:

a) consegna a mani presso l'Ufficio protocollo;
b) consegna via email all'indirizzo:
c) consegna via PEC all'indirizzo:

Ove al momento della rilevazione dell'incidente di sicurezza non sia possibile una descrizione particolareggiata dell'evento, è comunque essenziale procedere immediatamente alla sua segnalazione, anche con informazioni incomplete. Sarà cura del Titolare del trattamento accertare quanto necessario, anche contattando il segnalante ai recapiti forniti.

Dati identificativi del SEGNALANTE ed informazioni di contatto					
Cognome					
Nome					
Documento di identità N.		rilasciato da		scadenza	
Servizio o settore di appartenenza	(questo campo dev'essere compilato solo in caso di segnalazione ad opera di un dipendente/collaboratore del Titolare. In tale ipotesi non vanno indicati i riferimenti al documento di identità)				
Telefono		cellulare			
E-mail		PEC			

Informazioni sulla VIOLAZIONE	
Quando mi sono accorto della violazione?	
Come mi sono accorto della violazione?	

Breve **descrizione** della violazione	

Quali strutture sono coinvolte (locali, archivi, web, dispositivi elettronici, etc)?	

Quale tipo di violazione?	In caso di perdita di **confidenzialità**	
		I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
		I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
		I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
		Altro (specificare)
	In caso di perdita di **integrità**	
		I dati sono stati modificati e resi inconsistenti
		I dati sono stati modificati mantenendo la consistenza
		Altro (specificare)
	In caso di perdita di **disponibilità**	
		Mancato accesso a servizi
		Malfunzionamento e difficoltà nell'utilizzo di servizi
		Altro (specificare)

Quali soggetti coinvolti?		Il segnalante
		Cittadini
		Dipendenti e titolari di incarichi di collaborazione
		Utenti di servizi pubblici
		Soggetti che ricoprono cariche istituzionali
		Beneficiari o assistiti
		Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
		Minori
		Categorie ancora non determinate
		Altro (specificare)

Sono coinvolti cittadini di altri paesi?	(in caso affermativo, indicare i paesi di riferimento)

Quali dati personali sono coinvolti?		Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
		Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
		Dati di accesso e di identificazione (username, password, customer ID, altro...)
		Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...)
		Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro...)
		Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
		Dati di profilazione
		Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro...)
		Dati di localizzazione
		Dati che rivelino l'origine razziale o etnica
		Dati che rivelino opinioni politiche
		Dati che rivelino convinzioni religiose o filosofiche
		Dati che rivelino l'appartenenza sindacale
		Dati relativi alla vita sessuale o all'orientamento sessuale
		Dati relativi alla salute
		Dati genetici
		Dati biometrici
		Categorie ancora non determinate
		Altro, descrivere:

Quali potenziali effetti negativi per le persone coinvolte?		Perdita del controllo dei dati personali
		Limitazione dei diritti
		Discriminazione
		Furto o usurpazione d'identità
		Frodi
		Perdite finanziarie
		Decifratura non autorizzata della pseudonimizzazione
		Pregiudizio alla reputazione
		Perdita di riservatezza dei dati personali protetti da segreto professionale
		Conoscenza da parte di terzi non autorizzati
		Qualsiasi altro danno economico o sociale significativo (specificare)

È già stata fatta una segnalazione al Garante della privacy?	(in caso affermativo, allegare la relativa documentazione)
È già stata fatta una segnalazione alle forze dell'ordine o all'Autorità giudiziaria?	(in caso affermativo, allegare la relativa documentazione)

Documentazione che si allega	(diversa da quella indicata al punto precedente. Indicare anche eventuali fogli aggiuntivi necessari per ragioni di spazio)	
	X	Fotocopia del documento di identità (solo per soggetti esterni al Titolare)
Numero dei documenti allegati		

ANNOTAZIONI

Firma

_____, lì _____ _____

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che l'Ente di gestione delle Aree Protette delle Alpi Marittime, in qualità di Titolare del trattamento (con sede in Valdieri – CN, Piazza Regina Elena n. 30; Email: info@areeprotettealpimarittime.it; PEC: apam@pec.areeprotettealpimarittime.it), tratterà i dati personali conferiti con il presente modulo per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e s.m.i.), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri e, segnatamente, al solo scopo di acquisire ogni necessaria informazione in merito all'evento segnalato, adottare le conseguenti procedure di tutela ed effettuare le comunicazioni previste dalla normativa vigente.
Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio al fine della ricevibilità della segnalazione, ferma restando la facoltà del Titolare di istruire comunque il procedimento volto all'accertamento della violazione di dati personali. I dati acquisiti nell'ambito della procedura saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa. I dati saranno trattati esclusivamente dal personale e da collaboratori del Titolare o delle imprese espressamente designate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli al Garante per la protezione dei dati personali, all'Autorità giudiziaria e ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea. Gli interessati hanno il diritto di ottenere dal Titolare, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt.15 e ss. del Regolamento UE 2016/679). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati ai seguenti indirizzi (e-mail parco.alpimarittime.@gdpr.nelcomune.it; PEC: dpo@pec.gdpr.nelcomune.it). Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dalla disciplina in materia di protezione dei dati personali hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento (UE) 2016/679, o di adire le opportune sedi giudiziarie ai sensi dell'art. art. 79 del Regolamento citato.

ALLEGATO C

MODULO DI INOLTRO DI SEGNALAZIONE DI UNA POTENZIALE VIOLAZIONE DI DATI PERSONALI

ai sensi dell'art. 33 del Regolamento Generale sulla Protezione dei Dati

Ricevuta, da chiunque ed in qualunque modo, la segnalazione di un potenziale od effettivo incidente sulla sicurezza la medesima è immediatamente **trasmessa al Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta**, esclusivamente utilizzando il presente modulo, senza ritardo e, comunque, entro 4 ore dalla conoscenza dei fatti.

Il modello di segnalazione, debitamente compilato e sottoscritto, dovrà essere consegnato con le modalità più idonee (posta elettronica, consegna a mani, …) a garantirne la pronta e puntuale conoscenza in quanto permetterà di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso e, ciò, al fine di stabilire se si sia effettivamente verificata un'ipotesi di data breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto. Ove possibile, devono essere in questo modello integrate le informazioni richieste e non già fornite dal segnalante.

Contestualmente alla comunicazione scritta della segnalazione è necessario l'avvertimento del destinatario anche in modo verbale allo scopo di assicurarsi che quanto comunicato non passi inosservato.

Dati identificativi del soggetto che INOLTRA			
Cognome			
Nome			
Servizio o settore di appartenenza			
E-mail		Telefono	

Dati identificativi del soggetto DESTINATARIO				
Cognome				
Nome				
Servizio o settore di appartenenza				
E-mail			Telefono	
Modalità di inoltro segnalazione		A mani	data e ora	
		E-mail	data e ora	
		Avviso orale	data e ora	
		Altro (specificare)		

Informazioni sulla SEGNALAZIONE	
Da chi ho ricevuto la segnalazione?	

Quando ho ricevuto la segnalazione?	
Come ho ricevuto la segnalazione?	
(eventuali) ulteriori **informazioni** ricevute oralmente dal segnalante	

(eventuali) **Osservazioni** rispetto al contenuto della segnalazione ricevuta (anche in punto **descrizione** della violazione)	

ATTIVITA' DI RILEVAZIONE INTERNA

Competenza in merito alla segnalazione ricevuta (anche di più uffici)		Servizio o settore che l'ha ricevuta
		Altro/i servizio/i o settore/i (specificare)

Presenza di **Contitolari** del trattamento		NO
		SI (per ciascuno specificare denominazione e tipologia servizio affidato)

Presenza di **Responsabili** del trattamento		NO
		SI (per ciascuno specificare denominazione e tipologia servizio affidato)

istruttoria condotta con indicazione delle relative evidenze

Quale tipo di violazione?	In caso di perdita di **confidenzialità**	
		I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
		I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
		I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
		Altro (specificare)
	In caso di perdita di **integrità**	
		I dati sono stati modificati e resi inconsistenti
		I dati sono stati modificati mantenendo la consistenza
		Altro (specificare)

	In caso di perdita di **disponibilità**	
		Mancato accesso a servizi
		Malfunzionamento e difficoltà nell'utilizzo di servizi
		Altro (specificare)

Possibili **cause** della violazione		Azione intenzionale interna
		Azione accidentale interna
		Azione intenzionale esterna
		Azione accidentale esterna
		Sconosciuta
		Altro (specificare)

Volume (anche approssimativo) dei **soggetti** coinvolti		Numero
		Circa numero
		Numero (ancora) non definito (specificare)

Quali soggetti coinvolti?		Il segnalante
		Cittadini
		Dipendenti e titolari di incarichi di collaborazione
		Utenti di servizi pubblici
		Soggetti che ricoprono cariche istituzionali
		Beneficiari o assistiti
		Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
		Minori
		Categorie ancora non determinate
		Altro (specificare)

Sono coinvolti cittadini di altri paesi?	(in caso affermativo, indicare i paesi di riferimento)

Volume (anche approssimativo) dei **dati** coinvolti		Numero
		Circa numero
		Numero (ancora) non definito (specificare)

Quali dati personali sono coinvolti?		Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
		Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
		Dati di accesso e di identificazione (username, password, customer ID, altro...)
		Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...)
		Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro...)
		Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
		Dati di profilazione
		Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro...)
		Dati di localizzazione
		Dati che rivelino l'origine razziale o etnica
		Dati che rivelino opinioni politiche
		Dati che rivelino convinzioni religiose o filosofiche
		Dati che rivelino l'appartenenza sindacale
		Dati relativi alla vita sessuale o all'orientamento sessuale
		Dati relativi alla salute
		Dati genetici
		Dati biometrici
		Categorie ancora non determinate
		Altro, descrivere:

Quali potenziali effetti negativi per le persone coinvolte?		Perdita del controllo dei dati personali
		Limitazione dei diritti
		Discriminazione
		Furto o usurpazione d'identità
		Frodi
		Perdite finanziarie
		Decifratura non autorizzata della pseudonimizzazione
		Pregiudizio alla reputazione

		Perdita di riservatezza dei dati personali protetti da segreto professionale
		Conoscenza da parte di terzi non autorizzati
		Qualsiasi altro danno economico o sociale significativo (specificare)

Stima della **Gravità** della violazione		Trascurabile
		Basso
		Medio
		Alto
	Motivazione:	
AZIONI INTRAPRESE O SUGGERITE		

Misure tecniche ed organizzative adottate (o di cui si propone l'adozione) **per porre rimedio** alla violazione e ridurne gli effetti negativi per gli interessati	

Misure tecniche e organizzative adottate (o di cui si propone l'adozione) **per prevenire** simili violazioni future	

ALLEGATI E NOTE

Documentazione che si allega	X	Modulo di segnalazione di una potenziale violazione di dati personali e relativi allegati
Numero dei documenti allegati		

ANNOTAZIONI

Firma

_____, lì _____ _____

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che l'Ente di gestione delle Aree Protette delle Alpi Marittime, in qualità di Titolare del trattamento (con sede in Valdieri – CN, Piazza Regina Elena n. 30; Email: info@areeprotettealpimarittime.it; PEC: apam@pec.areeprotettealpimarittime.it), tratterà i dati personali conferiti con il presente modulo per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e s.m.i.), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri e, segnatamente, al solo scopo di acquisire ogni necessaria informazione in merito all'evento segnalato, adottare le conseguenti procedure di tutela ed effettuare le comunicazioni previste dalla normativa vigente.

Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio al fine della ricevibilità della segnalazione, ferma restando la facoltà del Titolare di istruire comunque il procedimento volto all'accertamento della violazione di dati personali. I dati acquisiti nell'ambito della procedura saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa. I dati saranno trattati esclusivamente dal personale e da collaboratori del Titolare o delle imprese espressamente designate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli al Garante per la protezione dei dati personali, all'Autorità giudiziaria e ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea. Gli interessati hanno il diritto di ottenere dal Titolare, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt.15 e ss. del Regolamento UE 2016/679). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati ai seguenti indirizzi (e-mail parco.alpimarittime.@gdpr.nelcomune.it; PEC: dpo@pec.gdpr.nelcomune.it). Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dalla disciplina in materia di protezione dei dati personali hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento (UE) 2016/679, o di adire le opportune sedi giudiziarie ai sensi dell'art. art. 79 del Regolamento citato.

ALLEGATO D

MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO ALLA VIOLAZIONE DI DATI PERSONALI

ai sensi dell'art. 33 del Regolamento Generale sulla Protezione dei Dati

Ricevuta la documentazione relativa alla segnalazione di una potenziale violazione di dati personali ed effettuata la prescritta analisi tecnica, il **Direttore ed eventuali altri dirigenti, competenti in relazione alla struttura coinvolta** devono stabilire la probabilità o meno che l'evento abbia comportato dei rischi per i diritti e la libertà delle persone e la gravità del rischio così identificato.

Il modello, debitamente compilato e sottoscritto, dovrà essere conservato a documentazione delle valutazioni e decisioni prese.

Dati identificativi del soggetto che effettua l'ANALISI				
Cognome				
Nome				
Servizio o settore di appartenenza				
E-mail			Telefono	
Ricevuta la segnalazione		A mani	data e ora	
		E-mail	data e ora	
		Avviso orale	data e ora	
		Altro (specificare)		

Dati identificativi del soggetto che effettua la VALUTAZIONE (se diverso)				
Cognome				
Nome				
Servizio o settore di appartenenza				
E-mail			Telefono	
Ricevuta la segnalazione		A mani	data e ora	
		E-mail	data e ora	
		Avviso orale	data e ora	
		Altro (specificare)		

ATTIVITA' DI ANALISI

Osservazioni rispetto al contenuto della segnalazione ricevuta	

(anche in punto **descrizione** della violazione)	

Data della violazione		il	
		Dal	(violazione ancora in corso)
		Dal	Al
		In un tempo non ancora determinato (specificare)	

Natura della violazione		**Riguarda dati personali**		**Non Riguarda dati personali**
		Perdita di confidenzialità		
		Perdita di integrità		
		Perdita di disponibilità		

Competenza in merito alla segnalazione ricevuta (anche di più uffici)		Servizio o settore che l'ha ricevuta
		Altro/i servizio/i o settore/i (specificare)

Presenza di **Contitolari** del trattamento		NO
		SI

Presenza di **Responsabili** del trattamento		NO
		SI

Descrizione dei **sistemi e delle infrastrutture IT coinvolti** nell'incidente, con indicazione della loro ubicazione e

Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti (**in essere** al momento della violazione)	

Possibili **cause** della violazione		Azione intenzionale interna
		Azione accidentale interna
		Azione intenzionale esterna
		Azione accidentale esterna
		Sconosciuta
		Altro (specificare)

Possibili conseguenze	In caso di perdita di **confidenzialità**

della violazione?		I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
		I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
		I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
		Altro (specificare)
	In caso di perdita di **integrità**	
		I dati sono stati modificati e resi inconsistenti
		I dati sono stati modificati mantenendo la consistenza
		Altro (specificare)
	In caso di perdita di **disponibilità**	
		Mancato accesso a servizi
		Malfunzionamento e difficoltà nell'utilizzo di servizi
		Altro (specificare)

Volume (anche approssimativo) dei **soggetti** coinvolti		Numero
		Circa numero
		Numero (ancora) non definito (specificare)

Quali soggetti coinvolti?		Il segnalante
		Cittadini
		Dipendenti e titolari di incarichi di collaborazione
		Utenti di servizi pubblici
		Soggetti che ricoprono cariche istituzionali
		Beneficiari o assistiti

		Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
		Minori
		Categorie ancora non determinate
		Altro (specificare)

Sono coinvolti cittadini di altri paesi?	(in caso affermativo, indicare i paesi di riferimento)

Volume (anche approssimativo) dei **dati** coinvolti		Numero
		Circa numero
		Numero (ancora) non definito (specificare)

Quali dati personali sono coinvolti?		Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
		Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
		Dati di accesso e di identificazione (username, password, customer ID, altro...)
		Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...)
		Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro...)
		Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
		Dati di profilazione
		Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro...)
		Dati di localizzazione

		Dati che rivelino l'origine razziale o etnica
		Dati che rivelino opinioni politiche
		Dati che rivelino convinzioni religiose o filosofiche
		Dati che rivelino l'appartenenza sindacale
		Dati relativi alla vita sessuale o all'orientamento sessuale
		Dati relativi alla salute
		Dati genetici
		Dati biometrici
		Categorie ancora non determinate
		Altro, descrivere:

Quali potenziali **effetti negativi** per le persone coinvolte?		Perdita del controllo dei dati personali
		Limitazione dei diritti
		Discriminazione
		Furto o usurpazione d'identità
		Frodi
		Perdite finanziarie
		Decifratura non autorizzata della pseudonimizzazione
		Pregiudizio alla reputazione
		Perdita di riservatezza dei dati personali protetti da segreto professionale
		Conoscenza da parte di terzi non autorizzati
		Qualsiasi altro danno economico o sociale significativo (specificare)

Stima della **Gravità** della violazione		Trascurabile (no notifica, né comunicazione)
		Basso (no notifica, né comunicazione)
		Medio (si notifica, no comunicazione)
		Alto e Molto Alto (si notifica e comunicazione)
	Motivazione:	

AZIONI INTRAPRESE O SUGGERITE

Misure tecniche e organizzative adottate (o di cui si propone l'adozione) **per prevenire** simili violazioni future	

ADEMPIMENTI

NOTIFICAZIONE ALL'AUTORITA' DI CONTROLLO

	Effettuata	in data e ora	

	No e non sarà effettuata in quanto si ritiene che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (specificare):

NOTIFICAZIONE O SEGNALAZIONE AD ALTRI ORGANISMI

Autorità giudiziaria			
	Effettuata	in data e ora	
	Modalità (specificare):		

Forze di polizia			
	Effettuata	in data e ora	
	Modalità (specificare):		

Altri organismi di vigilanza o controllo			
	Effettuata	in data e ora	
	Specificare l'organismo e le modalità di segnalazione		

COMUNICAZIONE AGLI INTERESSATI

	Effettuata	data e ora	
	Modalità e numero destinatari (specificare):		

	Non ancora effettuata
	in quanto tuttora in corso di valutazione
	Sarà effettuata in data da definire
	Sarà effettuata il

	No e non sarà effettuata in quanto:
	a) si ritiene che la violazione dei dati personali **non presenti un rischio elevato** per i diritti e le libertà delle persone fisiche (specificare):

	b) sono state **messe in atto le misure** tecniche ed 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 (specificare):
	c) sono state **successivamente adottate misure** atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati (specificare):
	d) detta comunicazione avrebbe richiesto **sforzi sproporzionati**. Gli interessati sono stati informati con altre modalità, quali:

ALLEGATI E NOTE

Documentazione che si allega	X	Modulo di segnalazione di una potenziale violazione di dati personali e relativi allegati
	X	Modulo di inoltro di una segnalazione di una potenziale violazione di dati personali e relativi allegati
	X	Copia notificazione all'Autorità di controllo (eventuale)
	X	Copia comunicazione agli interessati (eventuale)
Numero dei documenti allegati		

ANNOTAZIONI

Firma

_____, lì _____ _____

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che l'Ente di gestione delle Aree Protette delle Alpi Marittime, in qualità di Titolare del trattamento (con sede in Valdieri – CN, Piazza Regina Elena n. 30; Email: info@areeprotettealpimarittime.it; PEC: apam@pec.areeprotettealpimarittime.it), tratterà i dati personali conferiti con il presente modulo per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e s.m.i.), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri e, segnatamente, al solo scopo di acquisire ogni necessaria informazione in merito all'evento segnalato, adottare le conseguenti procedure di tutela ed effettuare le comunicazioni previste dalla normativa vigente.

Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio al fine della ricevibilità della segnalazione, ferma restando la facoltà del Titolare di istruire comunque il procedimento volto all'accertamento della violazione di dati personali. I dati acquisiti nell'ambito della procedura saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa. I dati saranno trattati esclusivamente dal personale e da collaboratori del Titolare o delle imprese espressamente designate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli al Garante per la protezione dei dati personali, all'Autorità giudiziaria e ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea. Gli interessati hanno il diritto di ottenere dal Titolare, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt.15 e ss. del Regolamento UE 2016/679). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati ai seguenti indirizzi (e-mail parco.alpimarittime.@gdpr.nelcomune.it; PEC: dpo@pec.gdpr.nelcomune.it). Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dalla disciplina in materia di protezione dei dati personali hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento (UE) 2016/679, o di adire le opportune sedi giudiziarie ai sensi dell'art. art. 79 del Regolamento citato.

ALLEGATO E

COMUNICAZIONE ALL'INTERESSATO DELLA VIOLAZIONE DEI DATI PERSONALI

(ai sensi del Regolamento Europeo 2016/679 sulla Protezione dei dati "GDPR")

(il presente modello costituisce una traccia liberamente modificabile e personalizzabile in considerazione delle circostanze di fatto coinvolte. Esso individua tuttavia il contenuto minimo che dev'essere in ogni caso garantito)

Gentile Signore/a,

Secondo quanto prescritto dall'articolo 34 del GDPR, La informiamo essersi verificato un accidentale ed imprevedibile evento che ha comportato una possibile violazione di dati dei Suoi dati personali.

Dagli accertamenti, tuttora in corso, è emerso che l'evento si sarebbe verificato in data _____, alle ore_____ e se ne è avuta conoscenza in data_____, alle ore_____.

DESCRIZIONE DELLA NATURA DELLA VIOLAZIONE

DOVE È AVVENUTA LA VIOLAZIONE

(Specificare ove sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

_____
_____
_____
_____

TIPO DI VIOLAZIONE

Per esempio: Lettura (presumibilmente i dati non sono stati copiati); Copia (i dati sono ancora presenti sui sistemi del Titolare); Alterazione (i dati sono 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)

_____
_____
_____
_____
_____

DISPOSITIVO OGGETTO DI VIOLAZIONE

Per esempio: Computer; Rete; Dispositivo mobile; Strumento di backup; Documento cartaceo

_____
_____
_____
_____

TIPO DI DATI OGGETTO DI VIOLAZIONE

Per esempio: Dati anagrafici (nome, cognome, telefono, mail, CF, indirizzo…); Dati di accesso e di identificazione (username, password, ID,…); Dati personali idonei a rivelare l'origine razziale ed etnica; Dati personali idonei a rivelare le convinzioni religiose; Dati personali idonei a rivelare convinzioni filosofiche o di altro genere; Dati personali idonei a rivelare le opinioni politiche; Dati personali idonei a rivelare l'adesione a partiti; Dati personali idonei a rivelare l'adesione a sindacati; Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso; Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere filosofico; Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere sindacale; Dati personali idonei a rivelare lo stato di salute; Dati personali idonei a rivelare la vita sessuale; Dati giudiziari; Dati genetici; Dati biometrici; Copia per immagine su supporto informatico di documenti analogici; Ancora sconosciuto.

_____

_____
_____
_____

Tale violazione è suscettibile di presentare un rischio elevato per Suoi diritti e le libertà.

DESCRIZIONE DELLE CONSEGUENZE DELLA VIOLAZIONE

_____
_____
_____
_____

DESCRIZIONE DELLE MISURE TECNOLOGICHE E ORGANIZZATIVE ASSUNTE

_____
_____
_____
_____

Per poter ottenere maggiori **informazioni** relativamente alla violazione in oggetto, può contattare lo scrivente Ufficio, nonché il Responsabile della Protezione dei Dati, i cui dati di contatto sono i seguenti: e-mail _____, PEC _____

Luogo e data

Firma

_____