DELIBERAZIONE DELLA GIUNTA REGIONALE 19 dicembre 2022, n. 1905

Procedura per la gestione degli eventi di violazione dei dati personali (c.d. Data Breach) ai sensi degli artt. 33 e 34 Regolamento UE 2016/679 (GDPR). Adozione.

Il Presidente della Giunta Regionale, sulla base dell'istruttoria espletata dal Responsabile P.O. "Protezione dati personali nel Sistema Regione" e confermata dal Dirigente della Sezione Affari istituzionali e giuridici, riferisce quanto segue:

Visti:

- la Deliberazione di Giunta Regionale n. 1518 del 31 luglio 2015 e successive modificazioni, con cui è stato adottato l'Atto di Alta Organizzazione del modello organizzativo denominato "*Modello Ambidestro per l'innovazione della macchina Amministrativa regionale MAIA*";
- la Deliberazione di Giunta Regionale n. 1974 del 7 dicembre 2020 e successive integrazioni e modifiche operate da ultimo con D.G.R. n. 1483 del 15 settembre 2021, recante approvazione del nuovo Modello Organizzativo regionale "MAIA 2.0", che sostituisce quello precedentemente adottato con D.G.R. n. 1518/2015 pur mantenendone i principi e criteri ispiratori, ed il conseguente Decreto del Presidente della Giunta Regionale n. 22 del 22 gennaio 2021, come modificato dal DPGR n. 45/2021 e successivi DPGR modificativi ed integrativi, recante adozione dell'Atto di alta organizzazione connesso al suddetto Modello organizzativo "MAIA 2.0".

Premesso che:

- Il Regolamento (UE) 2016/679 ("*General Data Protection Regulation*", d'ora innanzi GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato essenzialmente sulla valutazione dei rischi inerenti i diritti e le libertà degli interessati, ha riformato il precedente impianto normativo nazionale in materia di protezione dei dati personali (D.Lgs. 196/2003, cd. "Codice Privacy"), inserendo come elemento cardine il principio di *"accountability"* ("responsabilizzazione") posto in capo al Titolare del trattamento, nonché ad eventuali Responsabili, i quali sono tenuti a garantire la conformità al GDPR di tutte le attività di trattamento dati e la tutela dei diritti dell'interessato attraverso l'adozione di misure tecniche ed organizzative adeguate ed efficaci, sottoposte a continuo aggiornamento;
- Il D.Lgs. 101/2018 ha introdotto disposizioni per l'adeguamento del D.Lgs. n. 196/2003 "Codice Privacy" alle disposizioni del sopraccennato GDPR;
- Il GDPR detta una complessa disciplina di carattere generale, prevedendo molteplici obblighi e adempimenti in capo ai soggetti che trattano dati personali ed attribuendo, al tempo stesso, al Titolare del trattamento il compito di individuare le modalità operative per porre in essere i prescritti adempimenti;
- Fra gli adempimenti di maggiore rilevanza ci sono quelli connessi ad eventuali violazioni di dati personali, ossia a qualsiasi "*violazione di sicurezza che comporti - 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*", ai sensi degli artt. 33 e 34 del GDPR: il Titolare è tenuto alla notifica all'Autorità di Controllo (Garante per la protezione dei dati personali) senza ingiustificato ritardo – e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza – di ogni violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche; qualora la violazione comporti un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve darne notizia anche all'interessato senza ingiustificato ritardo. L'omessa notifica di *data breach* all'Autorità di Controllo, oltre a costituire un possibile danno per i soggetti interessati, è punita con l'irrogazione di sanzioni amministrative a carico del Titolare del trattamento;
- In caso di violazione, a mente del richiamato art. 33 GDPR, par. 5, il titolare del trattamento è altresì

tenuto a *"documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio"*, all'interno di apposito Registro delle violazioni;

- Specifiche "*Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679*", recanti illustrazione degli obblighi di notifica e comunicazione delle violazioni sanciti dal Regolamento nonché di alcune misure che i Titolari e i Responsabili del trattamento possono intraprendere per soddisfare questi nuovi obblighi, sono state adottate in data 3 ottobre 2017 ed emendate in data 6 febbraio 2018 dal Gruppo di lavoro per la protezione dei dati ex art. 29 (WP29), oggi Comitato Europeo per la Protezione dei Dati (EDPB);
- Successivamente, ancora più dettagliate "*Linee-guida n. 1/2021 su esempi riguardanti la notifica di una violazione dei dati personali*" sono state adottate dallo stesso EDPB in data 14 dicembre 2021.

Rilevato che:

- Con D.G.R. n. 145 del 30/1/2019 la Giunta Regionale della Puglia, in applicazione del disposto dell'art. 2-*quaterdecies* del D.Lgs. 101/2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679", ha delegato l'esercizio delle competenze del Titolare del trattamento in materia di protezione dei dati ai Dirigenti responsabili delle Strutture presso le quali si svolgono i singoli trattamenti, nominando questi ultimi "Designati del trattamento dei dati" e segnatamente definendone i relativi compiti.
- Sulla base delle previsioni della suddetta DGR n. 145/2019, i Dirigenti regionali – nella loro qualità di Designati al trattamento dei dati per le Strutture della Giunta regionale – sono tenuti, tra l'altro, a *"gestire i data breach*: *nei casi di violazioni di dati personali avvenuti anche presso responsabili "esterni" o loro eventuali sub-responsabili (per quanto attiene ai trattamenti di dati affidati), il designato al trattamento deve effettuare una prima necessaria istruttoria. Valutati i rischi per i diritti e le libertà delle persone fisiche, dovrà avvisare tempestivamente la struttura competente in materia di sicurezza informatica, il Titolare, il RPD e il Segretario Generale della Presidenza della Giunta Regionale, nonché implementare il Registro dei data breach. Sussiste l'obbligo di notifica e comunicazione di avvenuta violazione dei dati personali sia al Garante della Privacy che, in determinati casi, anche ai diretti interessati, entro 72 ore dal sinistro (art. 33)."*

Considerato che:

- Con D.G.R. n. 2297 del 9 dicembre 2019 la Giunta regionale ha designato il *Data Protection Officer* (DPO) della Regione Puglia, in sostituzione del precedente DPO nominato con DGR n. 794 del 15/5/2018;
- Con D.G.R. n. 794 del 15 maggio 2018 la Giunta regionale aveva già istituto un Gruppo di lavoro regionale per la protezione dei dati, con il compito di sorvegliare – a supporto del DPO – sull'osservanza della normativa in materia di tutela dei dati personali e di predisporre indicazioni affinché le Strutture regionali osservassero la normativa in materia;
- Con recente D.G.R. n. 663 del 11 maggio 2022 la Giunta regionale ha aggiornato ed integrato, tanto nelle funzioni quanto nella composizione, il suddetto Gruppo di lavoro istituito con D.G.R. n. 794/2018 *"in relazione alla complessità amministrativa e tecnologica del trattamento dei dati personali gestiti dalle Strutture regionali, nonché alla necessità di porre in essere azioni mirate e tempestive per la gestione di eventuali violazioni di dati personali ex art. 33 GDPR (data breach). In punto di funzioni, il sopraccennato Gruppo di lavoro oltre a vigilare sull'osservanza della normativa in materia di tutela dei dati personali e a predisporre indicazioni/direttive in materia rivolte alle Strutture di Giunta regionale, dovrà fornire supporto nell'analisi di dettaglio degli eventuali eventi di data breach (individuazione causa scatenante dell'evento; analisi dei possibili impatti per i diritti e le libertà dei soggetti interessati; ecc.) anche al fine di consentire una gestione rapida ed efficace della violazione*";
- Con successiva D.G.R. n. 1227 del 19 settembre 2022 la Giunta regionale ha ulteriormente integrato, al fine di garantirne la massima rappresentatività, la composizione del Gruppo di Lavoro regionale per la protezione dei dati personali, che pertanto risulta essere composto come di seguito:

- Responsabile Protezione Dati (RPD) della Regione Puglia;
- Responsabile P.O. "Protezione dati personali nel Sistema Regione";
- Responsabile P.O. "Responsabile dei sistemi informativi per l'AdA";
- Responsabile della Transizione al Digitale (RTD) della Regione Puglia;
- Amministratore di Sistema della Regione Puglia;
- Responsabile della Gestione documentale della Regione Puglia;
- Responsabile della Conservazione documentale della Regione Puglia;
- Responsabile della Protezione dei Dati della Società *in house* InnovaPuglia;
- Responsabile Sezione Data Center della Società *in house* InnovaPuglia;
- Dirigente della Sezione Trasformazione Digitale della Regione Puglia;
- Designato al trattamento *ex* DGR 145/2019 (ove presente) competente *ratione materiae* nella specifica questione oggetto di trattazione o coinvolto nella violazione di dati personali *ex* art. 33 GDPR verificatasi.

- Con la sopraccennata DGR n. 663/2022, facendo espresso riferimento al '*data breach*', è stato previsto che *"nell'ipotesi di violazione di dati personali ex art. 33 GDPR, le specifiche funzioni del Gruppo di lavoro in oggetto nonché le modalità e i tempi di relativa convocazione e di risoluzione della problematica – stante la ristrettezza dei termini fissati al riguardo dal GDPR – saranno oggetto di disposizioni di dettaglio nell'ambito di apposito atto deliberativo di Giunta Regionale in ordine alle procedure per la gestione di data breach".*

Ritenuto che:

- Si rende necessario dettare specifiche disposizioni procedurali in materia di violazione di dati personali ex artt. 33 e 34 del GDPR, definendo al tempo stesso gli assetti organizzativi in punto di attribuzione di compiti in materia all'interno della Regione Puglia, al fine di individuare le responsabilità dei diversi soggetti (interni ed esterni) coinvolti nel processo di *data breach* e di consentire all'Autorità Garante l'eventuale verifica del rispetto delle norme.

Si propone, pertanto, di approvare la Procedura per la gestione degli eventi di violazione dei dati personali (cd. *data breach*) della Regione Puglia, unitamente al relativo Registro delle violazioni, dandone ampia diffusione nei confronti di tutti i soggetti coinvolti.

Garanzie di riservatezza

La pubblicazione sul BURP, nonché la pubblicazione all'Albo o sul sito istituzionale, salve le garanzie previste dalla Legge 241/1990 in tema di accesso ai documenti amministrativi, avviene nel rispetto della tutela della riservatezza dei cittadini secondo quanto disposto dal Regolamento UE n. 679/2016 in materia di protezione dei dati personali, nonché dal D.Lgs. 196/2003 ss.mm.ii., ed ai sensi del vigente Regolamento regionale 5/2006 per il trattamento dei dati sensibili e giudiziari, in quanto applicabile. Ai fini della pubblicità legale, il presente provvedimento è stato redatto in modo da evitare la diffusione di dati personali identificativi non necessari ovvero il riferimento alle particolari categorie di dati previste dagli articoli 9 e 10 del succitato Regolamento UE.

VALUTAZIONE DI IMPATTO DI GENERE

La presente deliberazione è stata sottoposta a Valutazione di impatto di genere ai sensi della DGR n. 322 del 07/03/2022.

L'impatto di genere stimato è:

- ❏ diretto
- ❏ indiretto
- ☒ neutro

COPERTURA FINANZIARIA AI SENSI DEL D.LGS. 118/2011 s.m.i.

La presente deliberazione non comporta implicazioni, dirette e/o indirette, di natura economico-finanziaria e/o patrimoniale e dalla stessa non deriva alcun onere a carico del bilancio regionale.

Il Presidente, sulla base delle risultanze istruttorie come innanzi illustrate e motivate, ai sensi dell'art. 4, co. 4, lett. k) della L.R. n. 7/1997, propone alla Giunta Regionale:

- Di condividere quanto esposto in narrativa, che qui si intende integralmente riportato;
- Di approvare, in applicazione degli artt. 33 e 34 del GDPR, la "Procedura per la gestione degli eventi di violazione dei dati personali (cd. *data breach*) della Regione Puglia", allegata al presente atto deliberativo per farne parte integrante e sostanziale (Allegato A), unitamente al relativo Registro delle violazioni di dati personali (Allegato B);
- Di trasmettere il presente provvedimento ai Dirigenti della Regione Puglia nella loro qualità di Designati al trattamento, ai Referenti Privacy di tutte le Strutture regionali, ai componenti del "Gruppo di lavoro regionale per la protezione dei dati personali" di cui alla DGR n. 633/2022 come modificata dalla DGR n. 1127/2022;
- Di dare mandato ai Dirigenti della Regione Puglia, in qualità di Designati al trattamento, di dare massima diffusione al presente provvedimento nei confronti del proprio personale, al fine di massimizzare l'*accountability* dell'intera Amministrazione regionale sia per la prevenzione che per la gestione di eventi di violazione di dati personali;
- Di pubblicare il presente provvedimento sul Bollettino Ufficiale della Regione Puglia ai sensi della L.R. n. 13/1994 s.m.i.;
- Di pubblicare il presente provvedimento sul Portale web istituzionale regionale, all'interno della Sezione "Amministrazione Trasparente", Sottosezione "Disposizioni Generali/Atti generali/Atti amministrativi Generali".

I sottoscritti attestano che il procedimento istruttorio loro affidato è stato espletato nel rispetto della vigente normativa regionale, nazionale e comunitaria e che la seguente proposta di deliberazione, dagli stessi predisposto ai fini dell'adozione dell'atto finale da parte della Giunta regionale è conforme alle risultanze istruttorie.

Il Responsabile P.O. "Protezione dati personali nel Sistema Regione"
Dott.ssa Maria Lucatorto

Il Dirigente della Sezione Affari Istituzionali e Giuridici
Dott.ssa Rossella Caccavo

Il sottoscritto Segretario Generale del Presidente, ai sensi dell'art.18, comma 1, Decreto del Presidente della Giunta Regionale 22 gennaio 2021, n. 22 e ss.mm.ii., NON RAVVISA la necessità di esprimere osservazioni sulla presente proposta di DGR.

Il Segretario Generale della Presidenza
Dott. Roberto Venneri

Il Presidente della Giunta Regionale
Dott. Michele Emiliano

L A G I U N T A

- Udita la relazione e la conseguente proposta del Presidente;
- Viste le sottoscrizioni poste in calce alla proposta di deliberazione;

A voti unanimi espressi nei modi di legge

D E L I B E R A

- Di condividere quanto esposto in narrativa, che qui si intende integralmente riportato;
- Di approvare, in applicazione degli artt. 33 e 34 del GDPR, la "Procedura per la gestione degli eventi di violazione dei dati personali (cd. *data breach*) della Regione Puglia", allegata al presente atto deliberativo per farne parte integrante e sostanziale (Allegato A), unitamente al relativo Registro delle violazioni di dati personali (Allegato B);
- Di trasmettere il presente provvedimento ai Dirigenti della Regione Puglia nella loro qualità di Designati al trattamento, ai Referenti Privacy di tutte le Strutture regionali, ai componenti del "Gruppo di lavoro regionale per la protezione dei dati personali" di cui alla DGR n. 633/2022 come modificata dalla DGR n. 1127/2022;
- Di dare mandato ai Dirigenti della Regione Puglia, in qualità di Designati al trattamento, di dare massima diffusione al presente provvedimento nei confronti del proprio personale, al fine di massimizzare l'*accountability* dell'intera Amministrazione regionale sia per la prevenzione che per la gestione di eventi di violazione di dati personali;
- Di pubblicare il presente provvedimento sul Bollettino Ufficiale della Regione Puglia ai sensi della L.R. n. 13/1994 s.m.i.;
- Di pubblicare il presente provvedimento sul Portale web istituzionale regionale, all'interno della Sezione "Amministrazione Trasparente", Sottosezione "Disposizioni Generali/Atti generali/Atti amministrativi Generali".

Il Segretario Generale della Giunta
ANNA LOBOSCO

Il Presidente della Giunta
RAFFAELE PIEMONTESE

Allegato A

PROCEDURA PER LA GESTIONE DEGLI EVENTI DI VIOLAZIONE DEI DATI PERSONALI (CD. *DATA BREACH*) DELLA REGIONE PUGLIA

REGIONE PUGLIA

SOMMARIO

REGIONE PUGLIA

1. Premessa

Il Regolamento UE 679/2016 (Regolamento generale sulla protezione dei dati – GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, definisce la "violazione dei dati personali" come una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (c.d. "*data breach*").
A partire dal 25 maggio 2018, data in cui il sopraccennato Regolamento si applica in tutti gli Stati membri dell'Unione Europea, i Titolari del trattamento – pubblici e privati – devono notificare all'Autorità di controllo ("Garante") le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore dalla conoscenza delle stesse e comunque "senza ingiustificato ritardo", nel caso in cui ritengano probabile che da tali violazioni derivino rischi per i diritti e le libertà degli interessati (art. 33 GDPR).
La notifica all'Autorità Garante dell'avvenuta violazione pertanto non è obbligatoria in senso assoluto, ma risulta subordinata alla valutazione del rischio per i diritti e le libertà degli interessati, che spetta al Titolare o suo delegato. Se tale rischio sussiste, la notifica al Garante Privacy (GDPD) è obbligatoria; se la probabilità di tale rischio è elevata, si dovranno informare delle violazioni – oltre al GDPD – anche gli interessati (art. 34 GDPR).
Tutti i Titolari di trattamento sono tenuti, in ogni caso, a documentare tutte le violazioni di dati personali, anche se non notificate all'Autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (art. 33, par. 5, GDPR), all'interno di apposito Registro delle Violazioni, e sono altresì tenuti a fornire tale documentazione, su richiesta, al Garante Privacy in caso di accertamenti.

2. Finalità ed ambito di applicazione

La finalità del presente documento è quella di fornire informazioni generali sull'istituto della violazione di dati personali ed indicazioni operative di dettaglio che supportino i Dirigenti regionali, nella loro qualità di Designati al trattamento ex DGR 145/2019, per la segnalazione e gestione di eventuali violazioni di dati personali in applicazione degli artt. 33 e 34 GDPR.
Il presente documento si applica a tutti i trattamenti di dati personali di cui la Regione Puglia risulti Titolare, correlati ai procedimenti amministrativi che fanno capo alle varie Strutture regionali.

3. Definizione di violazione di dati personali

L'articolo 4, punto 12, del GDPR definisce la 'violazione dei dati personali' (cd. *data breach*) come una "*violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*".
Il Gruppo di lavoro ex articolo 29 per la protezione dei dati (WP29), oggi Comitato Europeo per la protezione dei dati (EDPB), nelle proprie "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" adottate il 3 ottobre 2017 ed integrate in data 6 ottobre 2018, in punto di definizioni chiarisce alcuni importanti aspetti interpretativi: "*Il significato di "distruzione" dei dati personali dovrebbe essere abbastanza chiaro: si ha distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento. Anche il concetto di "danno" dovrebbe essere relativamente evidente: si verifica un danno quando i dati personali sono stati modificati, corrotti o non sono più completi. Con "perdita" dei dati personali si dovrebbe invece intendere il caso in cui i dati potrebbero comunque esistere, ma il titolare del*

REGIONE PUGLIA

trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso. Infine, 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 regolamento".

Le Linee guida in oggetto riportano anche alcuni utili esempi, di seguito richiamati:

"Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei clienti del titolare del trattamento. Un altro esempio può essere il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un ransomware - programma informatico dannoso ("malevolo") che può "infettare" un dispositivo digitale - (malware del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso.

Ciò che dovrebbe essere chiaro è che una violazione è un tipo di incidente di sicurezza. Tuttavia, come indicato all'articolo 4, punto 12, il Regolamento 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'articolo 5 del Regolamento. 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".

La stessa Autorità Garante per la Protezione dei Dati Personali (GDPD) – nel proprio sito web istituzionale (https://www.garanteprivacy.it/regolamentoue/databreach) – elenca alcuni degli esempi più frequenti di violazione dati personali come di seguito:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

In sintesi, le violazioni di dati personali possono essere classificate in base ai tre principi fondamentali in materia di sicurezza delle informazioni:

- **Violazione della riservatezza/confidenzialità**, in caso di divulgazione dei dati personali o accesso agli stessi non autorizzato o accidentale;
- **Violazione dell'integrità**, in caso di modifica non autorizzata o accidentale dei dati personali;
- **Violazione della disponibilità**, in caso di perdita, impossibilità di accesso o distruzione accidentale o non autorizzata di dati personali.

A seconda dei casi, una violazione può riguardare anche contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Il Gruppo di lavoro ex art. 29, nelle richiamate Linee Guida, precisa al riguardo che *"mentre stabilire se vi sia stata una violazione della riservatezza o dell'integrità è relativamente evidente, può essere meno ovvio determinare se vi è stata una violazione della disponibilità. Una violazione sarà sempre considerata una violazione della disponibilità se si è verificata una perdita o una distruzione permanente dei dati personali".* Esempi di perdita di disponibilità – secondo quanto illustrato nelle medesime Linee Guida – "*possono aversi quando i dati vengono cancellati accidentalmente o da una persona non autorizzata, oppure, in caso di dati crittografati in maniera sicura, quando la chiave di decifratura viene persa. Se il titolare del trattamento non è in grado di ripristinare l'accesso ai dati, ad esempio ricorrendo a un backup, la perdita di disponibilità sarà considerata permanente. Può verificarsi perdita di disponibilità anche in caso di interruzione significativa del servizio abituale di un'organizzazione, ad esempio*

REGIONE PUGLIA

un'interruzione di corrente o attacco da "blocco di servizio" (denial of service) che rende i dati personali indisponibili" .

Una violazione può potenzialmente determinare numerosi effetti negativi significativi sulle persone fisiche, dai danni fisici a quelli materiali o immateriali. Il GDPR chiarisce che ciò può includere la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo per le persone fisiche interessate. Uno degli obblighi più importanti del Titolare del trattamento – e a cascata di ciascun dirigente Designato – risulta pertanto quello di valutare tali rischi per i diritti e le libertà degli interessati e attuare misure tecniche e organizzative adeguate per affrontarli.

Assume centralità, in tal senso, la questione delle misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, per la cui definizione ed attuazione – come previsto dall'art. 32 del Regolamento ("Sicurezza del trattamento") – si dovrebbe prendere in considerazione, tra l'altro, *"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"*.

4. Descrizione delle attività per la gestione dell'evento

In caso di segnalazione di una violazione di dati personali ai soggetti preposti al ricevimento della segnalazione (come specificati di seguito nel testo), occorre svolgere le seguenti attività per l'accertamento e l'eventuale notificazione:

- Analisi tecnica della violazione e contestuale messa in sicurezza;
- Valutazione dell'esistenza di un rischio o di un rischio elevato per i diritti e le libertà delle persone fisiche;
- Notifica al Garante Privacy, ove ricorrano i presupposti;
- Comunicazione agli interessati, se necessario;
- Inserimento dell'evento nel Registro delle Violazioni.

4.1 - Gestione del *data breach* da parte di Regione Puglia in qualità di Titolare del trattamento

I Dirigenti delle Strutture regionali, in qualità di Designati al trattamento ex DGR n. 145/2019 per le materie di rispettiva competenza, prendono in carico tutte le informazioni, notizie e/o segnalazioni interne o esterne relative a potenziali casi di *data breach*.

Ogni dipendente o collaboratore/consulente della Regione Puglia autorizzato a trattare i dati, qualora venga a conoscenza di un potenziale caso di *data breach*, anche tramite segnalazioni esterne dei cittadini-utenti, è tenuto ad avvisare tempestivamente il Dirigente della Struttura di appartenenza.

Il Dirigente della Struttura competente rispetto al trattamento di cui si ipotizza una violazione si attiverà senza ritardo per una valutazione preliminare e, qualora ravvisi la sussistenza di un'ipotesi di violazione di dati personali, procederà direttamente alla notifica della violazione al GDPD, dandone notizia al DPO regionale, oppure - in alternativa - darà segnalazione dell'ipotesi di violazione al DPO regionale ai fini di un'analisi e valutazione condivisa.

Il DPO regionale, ove coinvolto dal designato, procederà avvalendosi del "Gruppo di lavoro regionale per la protezione dei dati personali" istituito con DGR n. 663/2022 come integrata con successiva DGR n. 1277/2022, essendo attribuita a tale Gruppo, tra l'altro, la funzione di "*fornire supporto nell'analisi di dettaglio degli eventuali eventi di data breach (individuazione causa scatenante dell'evento; analisi dei possibili impatti per i diritti e le libertà dei soggetti interessati; ecc.) che interessino le Strutture di Giunta Regionale, anche al fine di consentire una gestione rapida ed efficace della violazione"*.

REGIONE PUGLIA

Il Dirigente trasmette la segnalazione al DPO mediante invio all'indirizzo di posta elettronica del Responsabile Protezione Dati regionale (*rpd@regione.puglia.it)*, specificando nell'oggetto: "Segnalazione presunto *data breach*".
La comunicazione al DPO, da effettuare tempestivamente, deve includere tutti i dettagli noti sull'incidente, con specifico riferimento a:

- Data e ora della violazione;
- Data e ora in cui è stata scoperta la violazione;
- Descrizione del tipo di violazione (accertata o presunta), degli ambiti di riferimento (violazione di riservatezza, integrità o disponibilità dei dati) e dell'oggetto specifico della violazione;
- Tipologia di dati coinvolti nella violazione (dati comuni, particolari categorie di dati, dati giudiziari);
- Modalità con cui è avvenuta la violazione, se note, avendo cura di evidenziare se la violazione è ancora in corso;
- Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione;
- Categoria/e di interessati coinvolti dalla violazione;
- Numero di interessati coinvolti, se noto, e dei dati personali di cui si presume il coinvolgimento;
- Azioni e misure di contenimento intraprese nell'immediatezza per porre rimedio alla violazione.
- Eventuale coinvolgimento di soggetti terzi (ad es. fornitori) cui siano imputabili le cause della violazione.

Per la suddetta comunicazione al DPO il Dirigente può utilizzare il modello (MODELLO PER LA SEGNALAZIONE DI VIOLAZIONI DI DATI PERSONALI) riportato in Appendice al presente documento.

Dal punto di vista dei tempi di gestione del *data breach*, il GDPR impone come già detto al Titolare del trattamento di notificare la violazione all'Autorità Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. Questo solleva la questione relativa al momento in cui il titolare del trattamento può considerarsi "a conoscenza" di una violazione.
Si richiamano sul punto le considerazioni effettuate dal Gruppo di lavoro ex articolo 29 per la protezione dei dati nelle "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679", nell'ambito delle quali *"il Gruppo di lavoro ritiene che il titolare del trattamento debba considerarsi 'a conoscenza' nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali (…). Il momento esatto in cui il titolare del trattamento può considerarsi 'a conoscenza' di una particolare violazione dipenderà dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, 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".*

Dunque, in caso di ipotesi di violazione di dati personali, il Dirigente regionale designato al trattamento, autonomamente o con il supporto di DPO e Gruppo di lavoro regionale in materia di protezione dei dati personali, con la massima tempestività dovrà:

- Analizzare tecnicamente l'evento, documentando adeguatamente il processo di analisi;
- Identificare gli eventuali *asset* da bonificare e tracciare le misure da porre in essere per risolvere le vulnerabilità;
- Rispettare gli obblighi di notifica e di comunicazione all'Autorità Garante, ed eventualmente agli interessati, ove ne ricorrano le condizioni;
- Annotare la violazione nel Registro delle Violazioni della Regione Puglia di cui al successivo par. 7 del presente documento.

4.2 - Gestione del *data breach* da parte del Responsabile del trattamento

Nel caso in cui attività e servizi che implicano un trattamento di dati personali vengano affidati dalla Regione Puglia a soggetti terzi, che assumono dunque il ruolo di Responsabili del trattamento *ex* art. 28

REGIONE PUGLIA

GDPR, il Dirigente Designato al trattamento *ratione materiae* è tenuto a stipulare con il Responsabile del trattamento un apposito Accordo di *Data Protection*.
Rispetto al configurarsi di ipotesi di *data breach* in tale situazione specifica, si richiama la disciplina contenuta nella D.G.R. n. 1328/2020 recante approvazione del modello di Accordo di *Data Protection ex* art. 28 GDPR: al punto 11 dell'art. 6 ("Obblighi del responsabile") di tale modello di Accordo, infatti, si stabilisce che il Responsabile è tenuto ad *"informare tempestivamente e, in ogni caso senza ingiustificato ritardo, il Titolare, nella persona del dirigente Designato, nonchè il DPO della Regione Puglia, rispetto all'avvenuta conoscenza di ogni violazione di dati personali (cd. Data breach) nell'ambito del trattamento in questione. Tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare, ove ritenuto necessario, di notificare la violazione all'Autorità Garante per la protezione dei dati personali entro il termine di 72 ore da quanto il medesimo Titolare ne venga a conoscenza. Nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Responsabile e/o di suoi eventuali sub-Responsabili".*
Come ha evidenziato il Gruppo di lavoro ex art. 29 per la protezione dei dati nelle già citate "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" dell'ottobre 2017, il Responsabile del trattamento non deve valutare la probabilità di rischio derivante dalla violazione prima di notificarla al Titolare del trattamento: *"spetta infatti a quest'ultimo effettuare la valutazione nel momento in cui viene a conoscenza della violazione. Il responsabile del trattamento deve soltanto stabilire se si è verificata una violazione e quindi notificarla al titolare del trattamento".*

Il Responsabile del trattamento, in sintesi, qualora venga a conoscenza di un potenziale caso di *data breach*, deve avvisare tempestivamente tanto il Titolare, nella persona del dirigente Designato con il quale ha stipulato l'accordo ex art. 28 (utilizzando la casella PEC – o mail in subordine – istituzionale del Designato), quanto il DPO regionale (utilizzando la casella mail del DPO - *rpd@regione.puglia.it*), avvalendosi del medesimo modello (MODELLO PER LA SEGNALAZIONE DI VIOLAZIONI DI DATI PERSONALI) utilizzato dal Designato per comunicare la violazione al DPO regionale e riportato in Appendice al presente documento. Nell'oggetto di entrambe le comunicazioni andrà sempre specificato che trattasi di "Segnalazione presunto *data breach*".
Il dirigente regionale Designato al trattamento, avvisato dal Responsabile del trattamento, rispetto alla violazione segnalata – con l'eventuale supporto del DPO regionale e del "Gruppo di lavoro regionale per la protezione dei dati personali" – dovrà porre in essere le medesime azioni indicate al precedente paragrafo 4.1.
E' fondamentale, in tal senso, che la procedura di segnalazione di *data breach* contenuta nel presente documento sia portata a conoscenza di tutti i Responsabili del trattamento, affinchè questi ultimi possano informare il Titolare Regione Puglia, nella persona del Designato al trattamento, senza ingiustificato ritardo, in tutte le ipotesi di violazione di dati personali.

4.3 – Analisi tecnica della violazione e contestuale messa in sicurezza

Il Dirigente della Struttura regionale coinvolta nella violazione, in qualità di Designato al trattamento, eventualmente supportato dal DPO regionale e dal "Gruppo di lavoro regionale per la protezione dei dati personali", dovrà condurre un'analisi tecnica della violazione volta ad accertare le circostanze e le caratteristiche della violazione, le conseguenze e i relativi rimedi. Ciò consentirà di stabilire se si sia effettivamente trattato di una "violazione", anche ai fini dell'eventuale notifica al Garante della Privacy, nonché di definire il grado di rischiosità dell'evento ai fini dell'eventuale comunicazione agli interessati.

Si specificano di seguito i passaggi di tale analisi tecnica della violazione:
Una volta rilevato un evento/incidente di sicurezza occorrerà analizzarlo, raccogliendo le principali informazioni relative alla potenziale violazione (data ed ora dell'evento, tipologia, dati e sistemi informativi coinvolti, numero e categoria di interessati coinvolti, ecc.) per poi classificare l'evento,

REGIONE PUGLIA

distinguendo tra violazione della confidenzialità, dell'integrità o della disponibilità dei dati personali secondo l'accezione già definita nel precedente paragrafo 3.
Effettuata l'individuazione e classificazione dell'evento, si provvederà alla valutazione delle cause che hanno provocato la violazione, oltre che degli eventuali impatti sulla confidenzialità, integrità e disponibilità dei dati personali e delle eventuali contromisure adottate nell'immediato per porvi rimedio.
Ciò consentirà di procedere alla qualificazione dell'evento/incidente di sicurezza come segue:

a) l'incidente non comporta alcuna violazione;
b) l'incidente comporta una violazione di dati personali. In questo caso, oltre a procedere all'annotazione della violazione nel Registro delle Violazioni della Regione Puglia, si dovrà stabilire se la violazione ricade nei casi in cui è necessario effettuare la notifica al Garante per la Protezione dei Dati Personali e se risulti altresì necessario – in base al livello di gravità – informare dell'accaduto l'interessato o gli interessati coinvolti nella violazione.

Nel corso dell'attività di analisi tecnica è altresì necessario procedere, ove si sia verificato un danno, al contenimento del medesimo ai fini della contestuale messa in sicurezza, adottando le contromisure idonee a ridurre al minimo i rischi e ad evitare future analoghe violazioni.
Il contenimento del danno è realizzato operando come di seguito:

- Limitazione degli effetti dell'incidente;
- Determinazione delle azioni possibili di ripristino e valutazione dei relativi tempi;
- Ripristino dei dati, dei sistemi e dell'infrastruttura;
- Valutazione delle eventuali vulnerabilità collegate con l'incidente;
- Individuazione delle azioni di mitigazione delle vulnerabilità individuate;
- Verifica dei sistemi recuperati;
- Raccolta delle eventuali prove in presenza di ipotesi di reato.

4.3 – Valutazione dell'esistenza di un rischio o di un rischio elevato per i diritti e le libertà delle persone fisiche.

L'analisi tecnica fin qui illustrata rappresenta il presupposto per la valutazione dell'esistenza di un rischio o di un rischio elevato per i diritti e le libertà delle persone fisiche, e dunque della gravità del danno derivante dalla violazione.
Si recepiscono, sul punto, le indicazioni del WP29 (ora EDPB), inserite nelle già citate "*Linee Guida sulla notifica delle violazioni dei dati personali*" del 2017 come integrate nel febbraio 2018, che al par. IV affrontano la tematica specifica della valutazione del rischio come riportato di seguito.

A. Rischio come fattore che fa scattare l'obbligo di notifica

Sebbene il Regolamento introduca l'obbligo di notificare una violazione, come già detto, non è obbligatorio farlo in tutte le circostanze:

- la notifica all'Autorità di controllo competente è obbligatoria a meno che sia improbabile che la violazione possa presentare **un rischio** per i diritti e le libertà delle persone fisiche;
- la comunicazione alle persone fisiche interessate diventa necessaria soltanto laddove la violazione possa presentare **un rischio elevato** per i diritti e le libertà delle persone fisiche.

Ciò significa che non appena il titolare del trattamento viene a conoscenza di una violazione, è fondamentale che non si limiti a contenere l'incidente, ma valuti anche il rischio che potrebbe derivarne. Questo per due motivi: innanzitutto conoscere la probabilità e la potenziale gravità dell'impatto sulle persone fisiche aiuterà il titolare del trattamento ad adottare misure efficaci per contenere e risolvere la violazione; in secondo luogo, ciò lo aiuterà a stabilire se è necessaria la notifica all'autorità di controllo e, se necessario, alle persone fisiche interessate.
In sintesi, la notifica di una violazione è obbligatoria a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche, mentre la comunicazione di una violazione agli interessati deve essere effettuata se è probabile che la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche. Tale rischio 'sussiste' quando la violazione può comportare un danno fisico, materiale o immateriale per le persone fisiche i cui dati sono stati violati:

REGIONE PUGLIA

esempi di tali danni sono la malattia o l'invalidità, il disagio psicologico, la discriminazione, il furto o l'usurpazione d'identità, le perdite finanziarie e il pregiudizio alla reputazione. Il verificarsi di tale danno dovrebbe essere considerato 'probabile' quando la violazione riguarda 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 (cfr. Considerando 75 e 85 GDPR).

B. Fattori da considerare nella valutazione del rischio

I considerando 75 e 76 del Regolamento suggeriscono che, di norma, nella valutazione del rischio si prenda in considerazione tanto la **probabilità** quanto la **gravità del rischio** derivante dalla violazione per i diritti e le libertà degli interessati.

Di conseguenza, nel valutare il rischio per le persone fisiche derivante da una violazione, il titolare del trattamento deve considerare tutte le circostanze specifiche della violazione, inclusa la gravità dell'impatto potenziale e la probabilità che tale impatto si verifichi, tenendo conto dei seguenti **fattori/criteri di valutazione del rischio**:

- **Tipo di violazione**

  Il tipo di violazione verificatosi può influire sul livello di rischio presentato per le persone fisiche.
  Ad esempio, una violazione della riservatezza che ha portato alla divulgazione di informazioni mediche a soggetti non autorizzati può avere conseguenze diverse per una persona fisica rispetto a una violazione in cui i dettagli medici di una persona fisica sono stati persi e non sono più disponibili.

- **Natura, carattere 'sensibile' e volume dei dati personali coinvolti**

  Elemento fondamentale della valutazione del rischio è rappresentato dal tipo e dal carattere 'sensibile' dei dati personali che sono stati compromessi dalla violazione.
  Generalmente più i dati sono sensibili, maggiore è il rischio di danni per le persone interessate. Tuttavia, in alcuni casi anche altri dati personali relativi all'interessato possono presentare un rischio elevato. Ad esempio, è improbabile che la divulgazione del nome e dell'indirizzo di una persona fisica in circostanze ordinarie causi un danno sostanziale; se però il nome e l'indirizzo di un genitore adottivo sono divulgati a un genitore biologico, le conseguenze potrebbero essere molto gravi tanto per il genitore adottivo quanto per il bambino.
  Violazioni relative a dati sulla salute, documenti di identità o dati finanziari come i dettagli di carte di credito, possono tutte causare danni di per sé, ma se tali dati fossero usati congiuntamente si potrebbe avere un'usurpazione d'identità. Di norma una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale.
  Alcuni tipi di dati personali possono sembrare relativamente innocui, ma occorre valutare attentamente ciò che questi dati possono rivelare sull'interessato. Un elenco di clienti che accettano consegne regolari potrebbe non essere particolarmente sensibile, tuttavia gli stessi dati relativi a clienti che hanno richiesto l'interruzione delle loro consegne durante le vacanze potrebbero essere informazioni utili per dei criminali.

- **Facilità di identificazione delle persone fisiche**

  Un fattore importante da considerare è la facilità con cui un soggetto che può accedere a dati personali compromessi riesce a identificare persone specifiche o ad abbinare i dati con altre informazioni per identificare persone fisiche. A seconda delle circostanze, l'identificazione potrebbe essere possibile direttamente dai dati personali oggetto di violazione senza che sia necessaria alcuna ricerca speciale per scoprire l'identità dell'interessato, oppure potrebbe essere estremamente difficile abbinare i dati personali a una particolare persona fisica, ma sarebbe comunque possibile a determinate condizioni. L'identificazione può essere direttamente o indirettamente possibile a partire dai dati oggetto di violazione, tuttavia può dipendere anche dal contesto specifico della

REGIONE PUGLIA

violazione e dalla disponibilità pubblica dei corrispondenti dettagli personali. Quest'ultima eventualità potrebbe essere più rilevante per le violazioni della riservatezza e della disponibilità.
Come indicato in precedenza, i dati personali protetti da un livello appropriato di cifratura saranno incomprensibili a persone non autorizzate che non dispongono della chiave di decifratura. Inoltre, anche una pseudonimizzazione opportunamente attuata (definita all'articolo 4, punto 5, del GDPR come "*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*") può ridurre la probabilità che le persone fisiche vengano identificate in caso di violazione. Tuttavia, le tecniche di pseudonimizzazione da sole non possono essere considerate sufficienti a rendere i dati incomprensibili.

- **Gravità delle conseguenze per le persone fisiche**

A seconda della natura dei dati personali coinvolti in una violazione (ad esempio, categorie particolari di dati) il danno potenziale alle persone che potrebbe derivarne può essere particolarmente grave, soprattutto se la violazione comporta furto o usurpazione di identità, danni fisici, disagio psicologico, umiliazione o danni alla reputazione.
Il fatto che il titolare del trattamento 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. Consideriamo una violazione della riservatezza nel cui ambito i dati personali vengono comunicati a un terzo di cui all'articolo 4, punto 10, o ad altri destinatari per errore. Una tale situazione può verificarsi, ad esempio, nel caso in cui i dati personali vengano inviati accidentalmente all'ufficio sbagliato di un'organizzazione o ad un'organizzazione fornitrice utilizzata frequentemente. Il titolare del trattamento può chiedere al destinatario di restituire o distruggere in maniera sicura i dati ricevuti. In entrambi i casi, dato che il titolare del trattamento ha una relazione continuativa con tali soggetti e potrebbe essere a conoscenza delle loro procedure, della loro storia e di altri dettagli pertinenti, il destinatario può essere considerato "affidabile". In altre parole, il titolare del trattamento può ritenere che il destinatario goda di una certa affidabilità e può ragionevolmente aspettarsi che non leggerà o accederà ai dati inviati per errore e che rispetterà le istruzioni di restituirli. Anche se i dati fossero stati consultati, il titolare del trattamento potrebbe comunque confidare nel fatto che il destinatario non intraprenderà ulteriori azioni in merito agli stessi e restituirà tempestivamente i dati al titolare del trattamento e coopererà per garantirne il recupero. In tali casi, questo aspetto può essere preso in considerazione nella valutazione del rischio effettuata dal titolare del trattamento in seguito alla violazione: in sostanza, il fatto che il destinatario sia affidabile può neutralizzare la gravità delle conseguenze della violazione, anche se questo non significa che non si sia verificata una violazione. La probabilità che detta violazione presenti un rischio per le persone fisiche verrebbe però meno, quindi non sarebbe più necessaria la notifica all'autorità di controllo o alle persone fisiche interessate. Ancora una volta, tutto dipenderà dalle circostanze del caso concreto.

- **Caratteristiche particolari dell'interessato**

Una violazione può riguardare dati personali relativi a minori o ad altre persone fisiche vulnerabili, che possono di conseguenza essere soggette a un rischio più elevato di danno. Altri fattori concernenti la persona fisica potrebbero influire sul livello di impatto della violazione sulla stessa.

- **Caratteristiche particolari del titolare del trattamento di dati**

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. Ad esempio, un'organizzazione medica tratterà categorie particolari di dati personali, il che significa che vi è una minaccia maggiore per le persone fisiche nel caso in cui i loro dati personali vengano violati, rispetto a una *mailing list* di un quotidiano.

REGIONE PUGLIA

- **Numero di persone fisiche interessate**

  Una violazione può riguardare solo una o poche persone fisiche oppure diverse migliaia di persone fisiche, se non molte di più. 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. Ancora una volta, l'aspetto fondamentale consiste nel considerare la probabilità e la gravità dell'impatto sulle persone interessate.

Pertanto, nel valutare il rischio che potrebbe derivare da una violazione secondo i criteri di cui innanzi, il Titolare del trattamento deve considerare tanto la gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche e quanto la probabilità che tale impatto si verifichi. Chiaramente, 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 è anche il rischio.

La valutazione del rischio, in forma schematica, produce il seguente esito:

		A	M	B
Probabilità	A			
	M			
	B			

Gravità

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

	Descrizione	**Notifica Garante**	**Comunicazione Interessati**
RISCHIO	Basso: nessun pregiudizio sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	No	No
	Medio: possibile pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	No
	Alto: pregiudizio certo sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	SI

In caso di dubbio sull'entità del rischio, il titolare del trattamento dovrebbe in via prudenziale effettuare comunque la notifica all'Autorità Garante.

Alcuni esempi utili relativi ai principali tipi di violazione di dati personali nell'ambito dell'attività istituzionale di Enti pubblici e privati – con l'indicazione se comportano o meno rischi o rischi elevati per

REGIONE PUGLIA

le persone fisiche, e dunque se necessitano di notifica all'Autorità Garante e di comunicazione all'interessato – sono stati forniti dalle medesime "*Linee Guida sulla notifica delle violazioni dei dati personali*" del WP29 (ora EDPB) del 2017, nel relativo Allegato B [link https://ec.europa.eu/newsroom/article29/items/612052[1]] e, successivamente, dalle ancor più dettagliate "*Linee-guida n. 1/2021 su esempi riguardanti la notifica di una violazione dei dati personali*" adottate il 14 dicembre 2021 dallo stesso EDPB [link https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_it].

Nell'ambito della metodologia fin qui descritta, per la valutazione del rischio relativo al trattamento di dati personali si procederà nel triennio 2023-2025 alla progettazione e messa a regime di un software applicativo regionale dedicato. Nelle more, è possibile utilizzare il cd. Tool ENISA, software messo a disposizione dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), la quale ha elaborato raccomandazioni in merito alla metodologia di valutazione della gravità di eventuali violazioni che possono essere utili per i titolari e responsabili del trattamento nella progettazione del loro piano di risposta per la gestione delle violazioni stesse[2].

5. Notifica all'Autorità di Controllo

Se a seguito della valutazione del rischio, operata secondo le indicazioni operative sin qui descritte, dovesse emergere la necessità di effettuare la notifica della violazione di dati al Garante Privacy ex art. 33 GDPR, il Titolare del trattamento, nella persona del Designato, provvederà alla notifica senza ingiustificato ritardo, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, tramite l'apposita procedura telematica disponibile sul portale dei servizi online dell'Autorità Garante, nella parte relativa alla "Compilazione della notifica" (https://servizi.gpdp.it/databreach/s/).

La notifica al Garante – secondo il fac-simile disponibile *on line* al link https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni – dovrà contenere i seguenti elementi:

- Descrizione della natura della violazione di dati personali, compresi, ove possibile, la/e categoria/e e il numero approssimativo dei dati personali in questione, nonché la/e categoria/e e il numero approssimativo di interessati coinvolti;
- Indicazione del nome e dei dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- Descrizione delle probabili conseguenze della violazione di dati personali;
- 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.

Qualora non sia possibile fornire tutte le informazioni necessarie contestualmente, come espressamente consentito dall'art. 33, co. 4, del GDPR*, "le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo*". Pertanto, sarà fondamentale raccogliere il maggior numero di informazioni e, anche nel caso in cui queste non siano ritenute esaustive, effettuare comunque la notificazione nei termini previsti, riservandosi successive integrazioni.

6. Comunicazione all'interessato

Nel caso in cui dalla valutazione del rischio, operata secondo le medesime indicazioni operative sin qui descritte, emergesse che la violazione in oggetto è "*suscettibile di presentare **un rischio elevato** per i*

[1] Download – *WP250_rev01_language_versions – Other (11.6 MB - ZIP).*

[2] ENISA, *Recommendations for a methodology of the assessment of severity of personal data breaches* [Raccomandazioni in merito a una metodologia di valutazione della gravità delle violazioni dei dati personali], https://www.enisa.europa.eu/publications/dbn-severity .

REGIONE PUGLIA

diritti e le libertà delle persone fisiche", il Titolare del trattamento, nella persona del Designato, è tenuto poi comunicare la violazione anche ai soggetti interessati ai sensi dell'art. 34 del GDPR.

La comunicazione all'interessato/agli interessati dovrà contenere almeno le seguenti informazioni:

- Una descrizione della natura della violazione e, laddove possibile, la/e categoria/e di dati personali impattati;
- I dati di contatto del Responsabile della protezione dei dati (DPO) o comunque del soggetto a cui sia possibile richiedere eventuali informazioni;
- Una descrizione delle conseguenze potenziali della violazione per l'interessato;
- Una descrizione delle misure messe in atto dal Titolare o delle misure che lo stesso intende adottare per rimediare alla violazione o per alleviarne gli effetti.

Per quanto attiene alle modalità di contatto, è preferibile l'utilizzo di un contatto diretto con il soggetto interessato, ad esempio tramite comunicazioni via e-mail o posta ordinaria, qualora ciò sia possibile e non comporti sforzi sproporzionati per il titolare. In alternativa, potranno essere previste misure che consentano comunque di informare i soggetti interessati, ad esempio attraverso comunicazioni sul sito web istituzionale del Titolare.

La comunicazione all'interessato non è richiesta nei seguenti casi :

a) Il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure sono 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 (ad es. 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 par. 1 dell'art. 34 del Regolamento;
c) Detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procederà con una comunicazione pubblica o misura simile, tramite la quale gli interessati siano informati con analoga efficacia.

7. Inserimento dell'evento nel Registro delle violazioni

Indipendentemente dalla valutazione relativa alla necessità di procedere o meno alla notifica al GDPD o alla comunicazione della violazione all'interessato, ogni qualvolta si verifichi una violazione di dati personali, la Regione sarà tenuta a documentarlo in applicazione dell'art. 33, par. 5, del GDPR a mente del quale "*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*".

Ai fini della suddetta documentazione, il Titolare del trattamento provvederà alla tenuta di un apposito Registro delle violazioni di dati personali, conservato presso l'Ufficio del DPO regionale e la cui compilazione sarà effettuata di volta in volta a cura del Dirigente Designato competente. Tale Registro è articolato secondo la struttura di cui all'Allegato B del presente atto deliberativo.

Nel Registro delle violazioni dovranno essere riportate le seguenti informazioni:

a. Oggetto della violazione;
b. Dirigente Designato ex DGR 145/2019;
c. Altri Soggetti Coinvolti nella violazione (Responsabile del trattamento/Contitolare del trattamento);
d. Data della violazione;
e. Data di conoscenza della violazione da parte del Titolare;
f. Breve descrizione della violazione;
g. Causa della violazione [Azione intenzionale interna; Azione accidentale interna; Azione intenzionale esterna; Azione accidentale esterna; Sconosciuta; Altro (specificare)];

REGIONE PUGLIA

h. Natura della violazione [Perdita di confidenzialità (diffusione/accesso non autorizzato o accidentale); Perdita di integrità (modifica non autorizzata o accidentale); Perdita di disponibilità (impossibilità di accesso, perdita, distruzione non autorizzata o accidentale)];
i. Sistemi, infrastrutture IT o banche dati coinvolti nella violazione;
j. Tipologia di dati personali violati [Dati comuni; Dati personali afferenti a particolari categorie (art. 9 GDPR); Dati personali relativi a condanne penali e reati (art. 10 GDPR)];
k. Effetti e conseguenze della violazione;
l. Misure tecniche ed organizzative adottate;
m. Notifica al Garante (Si/No);
n. Comunicazione agli Interessati (Si/No);
o. Motivazioni della mancata notifica o comunicazione;
p. Riferimento ad eventuali documenti utili (da allegare).

Anche per il Registro delle violazioni si procederà, nel triennio 2023-2025, alla progettazione e messa a regime di un software applicativo regionale dedicato. Nelle more, ciascun Dirigente Designato – rispetto alle violazioni che riguardino la Struttura di riferimento – provvederà a comunicare al DPO tutte le informazioni innanzi indicate ai fini della corretta e completa compilazione del Registro.

Il Registro delle violazioni sarà costantemente aggiornato e messo a disposizione dell'Autorità Garante, qualora la stessa chieda di accedervi.

REGIONE PUGLIA

APPENDICE _

MODELLO PER LA SEGNALAZIONE DI VIOLAZIONI DI DATI PERSONALI

Nominativo del soggetto che riporta l'incidente/violazione:

Ruolo del soggetto che riporta l'incidente/violazione: appartenenza al Titolare (Regione Puglia) o Contitolare (indicare la denominazione) o Responsabile del Trattamento (indicare la Denominazione) ovvero cittadino/interessato

_____

Dirigente Designato al trattamento dati:

_____

Eventuale coinvolgimento nella violazione di soggetti terzi (rispetto all'Ente Regione Puglia):

☐ SI, le cause della violazione sono imputabili a soggetti terzi/Responsabili del trattamento
☐ NO, le cause della violazione sono imputabili a soggetti interni all'Ente Regione

1) Quando si è verificata la violazione dei dati ?

Data: _____

Ora_____

2) Quando si è venuti a conoscenza della violazione dei dati ?

Data: _____

Ora_____

3) La violazione dei dati è (selezionare una sola opzione):

☐Accertata, sulla base dei seguenti elementi:

_____

☐Presunta, sulla base dei seguenti elementi

_____

REGIONE PUGLIA

4) La violazione dei dati riguarda (selezionare una o più opzioni):

☐ La riservatezza dei dati
☐ L'integrità dei dati
☐ La disponibilità dei dati

5) Descrizione/Oggetto della violazione :

_____

6) Dati coinvolti nella violazione (selezionare una o più opzioni e specificare i dati compromessi) :

☐ Dati personali comuni:

_____

☐ Categorie particolari di dati personali ex art. 9 GDPR (dati genetici o biometrici, dati relativi alla salute o alla vita sessuale, alle opinioni politiche, alle convinzioni religiose o filosofiche, all'appartenenza sindacale, ecc.):

_____

☐ Dati giudiziari ex art. 10 GDPR (dati relativi a condanne penali e reati) :

_____

7) Modalità in cui è avvenuta la violazione (se note), evidenziando se la violazione è ancora in corso;

_____

8) Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione :

_____

9) Categoria/e di soggetti interessati coinvolti :

_____

10) Numero dei soggetti interessati e dei dati personali di cui si presume il coinvolgimento (se noto):

_____

11) Azioni e misure di contenimento poste in essere nell'immediato :

_____

Allegato B)

Registro delle Violazioni di Dati Personali - REGIONE PUGLIA

Titolare del Trattamento	Regione Puglia
Indirizzo	Lungomare Nazario Sauro, 31-33
email	[illegible]
Pec	[illegible]

Responsabile della Protezione dei dati	RPD regione Puglia
Indirizzo	Lungomare Nazario Sauro, 31-33
email	[illegible]
Pec	

DETTAGLI DELLA VIOLAZIONE													**CONSEGUENZE**	**MISURE ADOTTATE**				
										Tipologia di dati personali violati								
Identificativo della Violazione	Oggetto della violazione	Dirigente Designato ex DGR 145/2019	Altri Soggetti Coinvolti nella violazione (Responsabile del trattamento/Contitolare del trattamento)	Data della Violazione	Data di conoscenza della violazione da parte del Titolare	Breve descrizione della violazione	Causa della Violazione *	Natura della Violazione **	Sistemi, infrastrutture IT o banche dati coinvolti nella violazione	Dati comuni	Dati personali afferenti a particolari categorie (art. 9 GDPR)	Dati personali relativi a condanne penali e reati (art. 10 GDPR)	Effetti e conseguenze della violazione	Misure Tecniche / Organizzative	Notifica al Garante (S/No)	Comunicazione agli interessati (S/No)	Motivazioni della mancata notifica o comunicazione	Link ipertestuali (eventuali) a documenti utili

LEGENDA	
* Causa della violazione	La causa della violazione - sulla base del Modello di Notifica reso disponibile dal Garante Privacy - va individuata fra le seguenti: Azione intenzionale interna; Azione accidentale interna; Azione intenzionale esterna; Azione accidentale esterna; Sconosciuta; Altro (specificare).
** Natura della violazione	La natura della violazione - sulla base del Modello di Notifica reso disponibile dal Garante Privacy - va individuata fra le seguenti: Perdita di confidenzialità (diffusione/accesso non autorizzato o accidentale); Perdita di integrità (modifica non autorizzata o accidentale); Perdita di disponibilità (impossibilità di accesso, perdita, distruzione non autorizzata o accidentale).

Rossella Caccavo
12.12.2022
13:18:46
GMT+00:00