SISTEMA DI GESTIONE DEI DATI PERSONALI
Procedura di gestione dei data breach
ai sensi del Regolamento UE 2016/679

SCOPO E CAMPO DI APPLICAZIONE

Scopo della presente procedura è descrivere compiti e responsabilità nel processo di gestione delle violazioni dei dati personali (c.d. *data breach*) nel rispetto delle disposizioni contenute nel Regolamento europeo n. 2016/679 (General Data Protection Regulation, di seguito GDPR).

Tale processo si sviluppa nelle seguenti fasi:

a) Rilevazione e inquadramento dell'incidente di sicurezza;
b) Messa in atto delle strategie di contenimento dei rischi e delle eventuali azioni correttive;
c) Svolgimento di ulteriore attività investigativa volta a individuare le conseguenze e/o i possibili rischi per i diritti e le libertà delle persone fisiche;
d) Eventuale notificazione del data breach all'Autorità Garante ai sensi dell'art. 33 GDPR e in conformità con le previsioni della WP 250 del 6 febbraio 2018;
e) Eventuale comunicazione agli Interessati coinvolti, quando la violazione dei dati personali presenta un rischio elevato per i loro diritti e libertà;
f) Registrazione dell'evento ai sensi dell'art. 33, par. 5, GDPR, al fine di documentare qualsiasi violazione dei dati personali comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale attività non ha solo una finalità di compliance, ma anche di analisi interna per l'apprendimento e il miglioramento continuo delle misure di sicurezza, al fine di prevenire il ripetersi di incidenti analoghi, come sottolineato dalle linee guida dell'European Data Protection Board (EDPB).

RIFERIMENTI NORMATIVI

La presente procedura risponde ai seguenti requisiti normativi:

1. Regolamento UE 2016/679 "Regolamento generale sulla protezione dei dati personali":
   - art. 24 e 25 GDPR - Responsabilizzazione (accountability) e Protezione dei dati fin dalla progettazione e per impostazione predefinita (by design e by default), principi cardine per una corretta prevenzione.
   - art. 32 GDPR - Sicurezza del trattamento, che impone l'adozione di misure tecniche e organizzative adeguate a prevenire le violazioni.
   - art. 33 GDPR - Notifica di una violazione dei dati personali all'autorità di controllo;
   - art. 34 GDPR - Comunicazione di una violazione dei dati personali all'interessato.
2. Decreto legislativo n. 196/2003 "Codice in materia di protezione dei dati personali", come modificato dal D.Lgs. n.101/2018.
3. Linee Guida in materia di notifica delle violazioni dei dati personali - WP250 rev.01 e le successive Guidelines 01/2021 on Examples regarding Personal Data Breach Notification dell'EDPB, che forniscono esempi pratici di valutazione del rischio.
4. Provvedimenti emessi dall'Autorità Garante e, in particolare, il Provvedimento n. 393 del 2 luglio 2015 – "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche" e relativo Allegato 1 "Modello di comunicazione al Garante".
5. La giurisprudenza della Corte di Giustizia dell'Unione Europea e delle corti nazionali, che chiarisce aspetti fondamentali come la nozione di danno risarcibile e l'onere della prova.

ACRONIMI E DEFINIZIONI UTILIZZATE

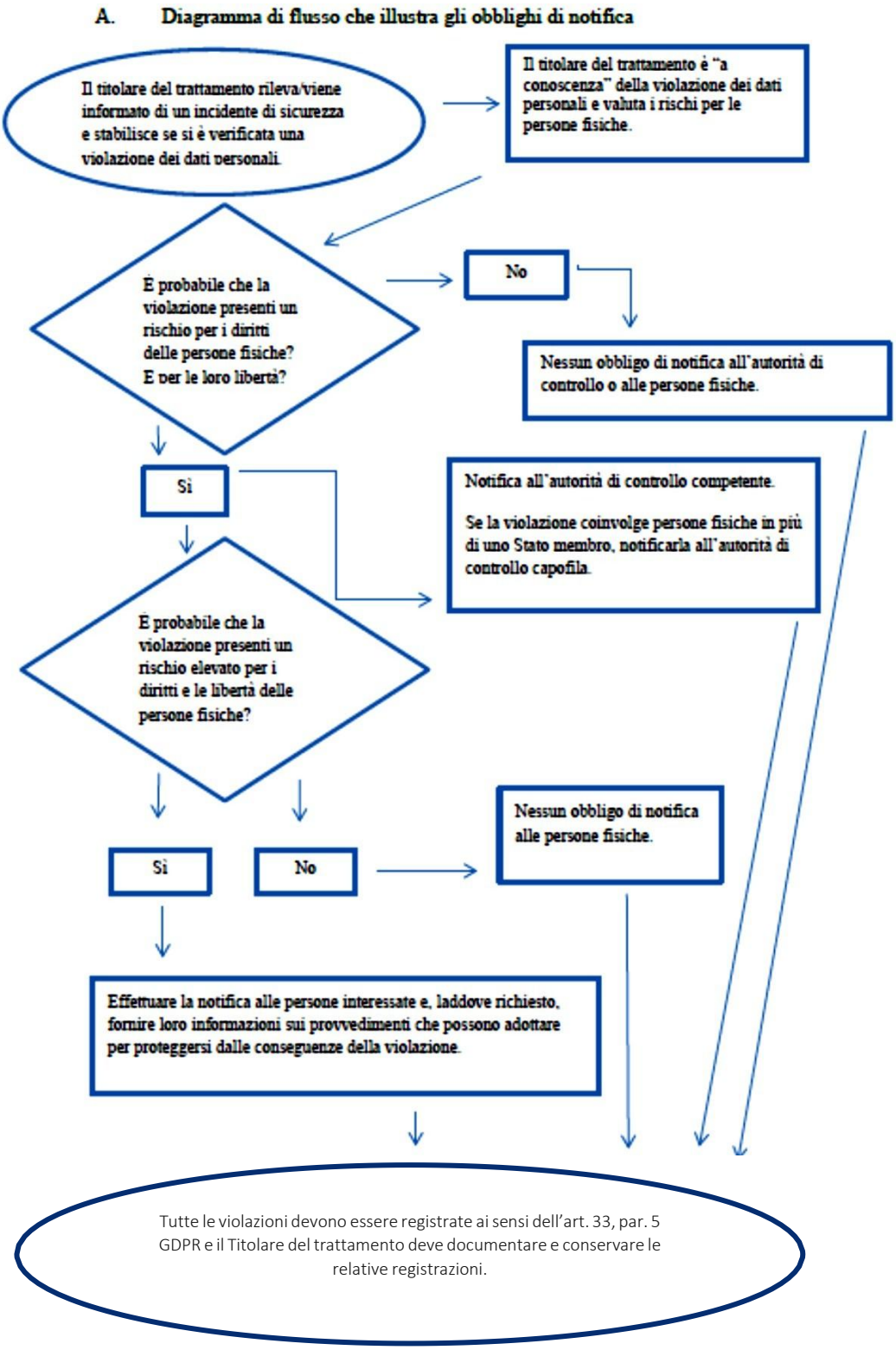
GDPR	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice Privacy	D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018
Garante	Autorità Garante per la protezione dei dati personali
WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo della protezione dei dati) – EDPB (European Data Protection Board)
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
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 (art. 4, punto 7 del GDPR)
DPO/ RPD	Data Protection Officer / Responsabile della protezione dei dati ai sensi dell'art. 37 del GDPR
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, ai sensi dell'art. 4, punto 8 del GDPR
Referente Privacy	Persona nominata per coordinare le attività in ambito di privacy
Amministratore di Sistema	Persona fisica incaricata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, ivi comprese le figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi
RL	Rappresentante Legale dell'Ordine
Incidente di sicurezza	Qualsiasi accadimento significativo per la gestione delle infrastrutture IT e per la gestione dell'operatività dei servizi
Violazione dei dati (data breach)	L'incidente 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 (art. 4, punto 12 GDPR). Come chiarito dall'EDPB, una violazione può essere classificata in base a tre principi: • "*Violazione della riservatezza*": divulgazione o accesso non autorizzato o accidentale a dati personali. • "*Violazione dell'integrità*": modifica non autorizzata o accidentale di dati personali. • "*Violazione della disponibilità*": perdita dell'accesso, distruzione accidentale o non autorizzata di dati personali. Un singolo incidente può coinvolgere una o più di queste categorie contemporaneamente.

MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Stato	Descrizione	Approvazione

FASI DEL PROCESSO

La gestione di un data breach può riassumersi nelle fasi di seguito rappresentate.



N.B. Il Titolare del trattamento si considera "a conoscenza" della violazione, e da quel momento decorre il termine di 72 ore per la notifica, non dal primo sospetto, ma dal momento in cui, a seguito di una breve indagine iniziale, acquisisce un grado di certezza ragionevole che si sia verificato un incidente di sicurezza che ha compromesso i dati personali. Questo, come specificato dal Garante nel Provvedimento del 27 gennaio 2022, Ordinanza ingiunzione nei confronti di Azienda sociosanitaria territoriale Nord di Milano, permette di distinguere la fase investigativa preliminare dall'avvenuta conoscenza che fa scattare gli obblighi di notifica.

RILEVAZIONE E INQUADRAMENTO DELL'INCIDENTE DI SICUREZZA e ATTIVITA' DI REMEDIATION IMMEDIATE

La rilevazione di un incidente può avvenire da diverse fonti:

↘ **SEGNALAZIONE AUTOMATICA**: sistemi di segnalazione automatica (es. SIEM - *Security Information and Event Management*), come le violazioni derivanti da superamento dei sistemi di Firewall dell'Ordine.

↘ **SEGNALAZIONE INTERNA**: attività di monitoraggio degli eventi da parte dei tecnici/dell'Amministratore di sistema; comunicazione di: malfunzionamenti irrituali o blocco dei sistemi, furti, smarrimenti, intrusioni fisiche nei locali archivio, etc.

↘ **SEGNALAZIONE ESTERNA**: da parte di Responsabili esterni nominati ai sensi dell'art. 28 GDPR, di fornitori esterni e/o altri consulenti nell'ambito dell'attività di monitoraggio, assistenza e manutenzione prestata a favore dell'Ordine, ovvero di utenti dei servizi e/o dei cittadini.

A tutti i soggetti che trattano dati per conto dell'Ordine, quali Responsabili Esterni del Trattamento, devono essere imposti contrattualmente almeno i seguenti obblighi:

- comunicare al Referente contrattuale interno eventuali incidenti di sicurezza che abbiano coinvolto i dati oggetto di trattamento, specificando le azioni correttive poste in essere e gli esiti delle stesse;
- fornire, in caso di necessità, anche attraverso il proprio RPD (ove nominato), la massima disponibilità e collaborazione per l'adempimento di tutti gli obblighi di cui agli artt. 32 e 36 GDPR.

Tutte le segnalazioni ricevute dall'Ordine, relative a incidenti di sicurezza devono essere inoltrate ai referenti dell'attività interessata dall'evento. Questi devono coinvolgere immediatamente il Referente Privacy interno.

Il Referente Privacy:

a) attiva:
- il Responsabile Area IT ove l'evento riguardi l'infrastruttura, sistemi informativi/banche dati gestite internamente all'Ordine;
- il Referente delle altre parti coinvolte nell'incidente di sicurezza segnalato.

b) assume ogni informazione utile a inquadrare la tipologia dell'incidente e, conseguentemente, accerta se tale evento ha coinvolto o meno dati personali. In particolare, devono essere definiti:
1. il sistema, infrastruttura, applicazione, banca dati oggetto dell'incidente di sicurezza;
2. la tipologia dell'evento verificatosi (violazione della riservatezza/ dell'integrità /della disponibilità dei dati);
3. il volume dei dati e laddove possibile il numero degli interessati coinvolti;
4. le misure di sicurezza applicate;
5. le attività di remediation (azioni correttive) immediate;
6. le attività di remediation (azioni correttive) ipotizzabili e/o future affinché lo stesso evento non si ripeta più.

c) pone in essere tutte le necessarie strategie di contenimento dei rischi e le eventuali azioni di remediation (azioni correttive) immediate, anche in collaborazione con il referente dell'attività interessata dall'evento.

d) relaziona sull'incidente di sicurezza e sulle misure di remediation ipotizzabili e/o future al RL per ogni più opportuna decisione.

Nel caso in cui l'evento coinvolga dati personali, viene attivata la successiva fase che comporta lo svolgimento di attività investigativa volta ad individuare i possibili rischi per i diritti e le libertà delle persone fisiche, la segnalazione dell'evento al RPD e la costituzione del Team per il caso di specie.

SVOLGIMENTO DI ATTIVITÀ INVESTIGATIVA VOLTA AD INDIVIDUARE LE CONSEGUENZE E/O I POSSIBILI RISCHI PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE

Dopo aver assunto tutte le informazioni di cui al punto precedente, ove l'incidente sia stato qualificato come *data breach*, il Referente Privacy segnala l'evento a:

- RPD dell'Ordine;
- Referente dell'attività coinvolta nella violazione di dati;
- Responsabile Area IT ove l'evento riguardi l'infrastruttura, sistemi informativi/banche dati gestite internamente all'Ordine;
- Referente del Responsabile Esterno che ha realizzato/fornito il prodotto/servizio interessato dal *data breach* e/o il suo RPD (ove nominato).

Questi ultimi devono individuare le possibili conseguenze per i diritti e le libertà delle persone fisiche, valutarne la gravità e definire le misure da adottare nell'immediato in risposta all'emergenza al fine di contenere gli effetti negativi.

La valutazione del rischio per i diritti e le libertà degli interessati deve essere oggettiva e tenere conto sia della probabilità che della gravità del rischio. I fattori da considerare, come indicato in numerosi provvedimenti del Garante (ad esempio, Provvedimento del 9 maggio 2024), includono:

- La natura della violazione (es. attacco hacker, errore umano, smarrimento).
- Le categorie e la quantità di dati personali coinvolti (es. dati anagrafici, dati particolari come quelli sanitari, dati finanziari, credenziali di accesso).
- La facilità di identificazione degli interessati.
- La gravità delle possibili conseguenze, quali furto o usurpazione d'identità, perdite finanziarie, danno reputazionale, perdita di controllo sui propri dati o discriminazione.
- Il numero di interessati coinvolti.

A tal fine:

a) ove disponibili sono raccolte, consolidate e/o approfondite le informazioni di cui al format per la comunicazione al Garante (***All. 1***);

b) successivamente, sono effettuate le seguenti valutazioni circa:

- la natura della violazione dei dati personali e, ove possibile, le categorie dei dati e il numero (anche solo) approssimativo degli interessati coinvolti (**c.d. gravità dell'accadimento**);
- le possibili/probabili conseguenze della violazione accertata dei dati personali rispetto ai diritti ed alle libertà dell'interessato (ad esempio in termini di danno fisico, materiale o immateriale quali perdita del controllo dei dati personali o limitazione dei loro diritti; 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; qualsiasi altro danno economico o sociale) (**valutazione dell'entità dei possibili danni agli interessati**);
- la valutazione dell'adeguatezza delle misure di sicurezza già implementate da parte del Titolare (o del Responsabile del trattamento) per porre rimedio alla violazione e per attenuare i possibili effetti negativi e/o probabili danni agli interessati.
- le possibili azioni correttive da adottare nell'immediato al fine di contenere gli effetti negativi e minimizzare il possibile danno agli interessati.

Per la definizione dell'impatto sui diritti e le libertà degli interessati si fa riferimento ai livelli di rischio individuati dal manuale sulla sicurezza nel trattamento dei dati personali (rev. 12/2017) "ENISA" riportati nella seguente tabella:

GRAVITÀ	RISCHIO	DESCRIZIONE
Minore di 2	Basso	Gli interessati non incontreranno inconvenienti o potrebbero incontrare alcuni inconvenienti che supereranno senza alcun problema (tempo passato a reinserire informazioni, fastidio, irritazione, ecc.)
Compreso tra 2 e 3	Medio	Gli interessati potranno incontrare inconvenienti significativi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici lievi, ecc.)
Compreso tra 3 e 4	Alto	Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione, peggioramento della salute, ecc.)
Maggiore di 4	Molto alto	Gli interessati possono incontrare conseguenze significative o addirittura irreversibili che non possono superare (difficoltà finanziarie come debito sostanziale o incapacità al lavoro, disturbi psicologici a lungo termine o disturbi fisici, morte, ecc.)

Ad esito dell'analisi:

a) nel caso in cui risulti improbabile – anche in considerazione dell'adeguatezza delle misure correttive adottate – che la violazione presenti un rischio per i diritti e le libertà degli Interessati, il Referente Privacy provvede a verbalizzare gli esiti dell'analisi riportando esplicitamente il parere formalizzato dal RPD ed aggiorna il Registro dei Data breach come da format allegato (***All. 3***);
Copia del verbale deve essere inviata al RPD e al RL, che, se del caso, riferirà l'accaduto al Consiglio dell'Ordine e adotterà ogni altro opportuna decisione di sua competenza.

b) nel caso risulti che la violazione possa comportare un rischio per i diritti e le libertà degli interessati, il Referente Privacy provvede a:

   - definire ed assegnare responsabilità e tempistiche per le azioni correttive individuate anche verso i Responsabili Esterni coinvolti;
   - verbalizzare gli esiti dell'analisi riportando esplicitamente il parere formalizzato dal RPD;
   - compilare o completare il Modello per la notificazione al Garante (***All. 1***) indicando esplicitamente se le azioni correttive previste sono già concluse od ancora *in itinere.*

c) nel caso risulti che la violazione possa comportare un elevato rischio per i diritti e le libertà degli interessati, fermo quanto previsto al punto precedente, il Referente privacy compila anche il Modello per la comunicazione della violazione agli interessati (vedasi ***All. 2***) e, in accordo con il RPD, individua le modalità più opportune con le quali effettuare tale comunicazione.

d) nelle ipotesi di cui ai precedenti punti b) e c), il Referente Privacy invia il verbale riportante gli esiti dell'analisi dei rischi sui diritti e le libertà delle persone fisiche, al Consiglio dell'Ordine al quale spetta la decisione finale di procedere o meno alla notificazione all'Autorità Garante e se del caso alla comunicazione della violazione agli stessi Interessati. Il RL deve riferire al Consiglio dell'Ordine in merito al data breach occorso e alla gestione dello stesso.

NOTIFICAZIONE DEL DATA BREACH ALL'AUTORITA' GARANTE PER LA PROTEZIONE DEI DATI PERSONALII

Il Titolare del trattamento una volta venuto a conoscenza del data breach deve notificare l'accaduto all'Autorità Garante a mezzo di compilazione del Modello di cui all'***All. 1***, debitamente sottoscritto con firma digitale dal RL ed inviato nel più breve tempo possibile, **possibilmente entro 72 ore** dall'avvenuta conoscenza**.**

È cruciale che la notifica non sia tardiva o incompleta. Il Garante, come nel Provvedimento del 4 luglio 2024, ha sanzionato titolari per notifiche prive degli elementi essenziali richiesti dall'articolo 33, paragrafo 3, del GDPR, in quanto una notifica carente impedisce all'Autorità di svolgere le proprie funzioni di vigilanza. La notifica non deve essere ritardata in attesa di un'analisi forense completa; è possibile e doveroso procedere con una notifica iniziale, anche parziale, da integrare successivamente non appena disponibili ulteriori informazioni, come previsto dall'articolo 33, paragrafo 4, del GDPR e chiarito dalle linee guida EDPB.

L'Ordine in qualità del Titolare del trattamento deve considerarsi "a conoscenza" del *data breach* nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali trattati nell'ambito della propria attività.

Ove la notifica avvenga oltre tale limite temporale – in particolare, in caso di data breach particolarmente complesso e/o di serie di attacchi/violazioni consecutive che necessitano di una indagine complessa – è necessario dare conto delle ragioni / motivi che hanno comportato il ritardo.

Qualora non si disponga di tutte le informazioni previste dal format (*All.1*), è possibile inviare una prima notifica parziale, da completare non appena disponibili le ulteriori informazioni. Se dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione dei dati personali, l'Azienda può chiedere all'Autorità Garante la cancellazione/revoca della notifica eseguita e l'incidente sarà registrato come un evento che non costituisce data breach.

Contestualmente alla notifica il Referente privacy aggiorna il "Registro dei Data Breach" (*All.3*)

COMUNICAZIONE DEL DATA BREACH AGLI INTERESSATI COINVOLTI

Come specificato dal Considerando 86 del GDPR, lo scopo primario della comunicazione agli interessati è consentire loro di adottare le necessarie precauzioni per proteggersi e mitigare i potenziali effetti negativi della violazione (ad esempio, cambiando le password, monitorando i propri conti bancari, prestando attenzione a tentativi di phishing). Per questo motivo, la comunicazione deve avvenire "senza ingiustificato ritardo", ovvero il prima possibile.

Nei casi in cui il RL, valutato il verbale riassuntivo delle indagini svolte ricevuto dal Referente Privacy, riscontri la necessità di comunicare il data breach agli interessati in quanto la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche, ne dà comunicazione al Referente Privacy.

Il Referente Privacy, successivamente:

- provvede a definire la comunicazione agli interessati che deve essere formulata con linguaggio chiaro e semplice e deve contenere tutti i seguenti elementi:
  - la natura della violazione dei dati personali;
  - le probabili conseguenze della violazione dei dati personali;
  - le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione;
  - il nome e i dati di contatto del responsabile della protezione dei dati.

- in accordo con RPD, definisce le modalità di comunicazione agli interessati:
  - invio della comunicazione a ciascun interessato, ove sia tecnicamente possibile reperirne i dati di contatto e l'attività possa essere sostenuta senza sforzi sproporzionati (ad es., disponibilità di email/pec);
  - comunicazione pubblica/generalizzata (ad es., pubblicazione in evidenza sul sito istituzionale, comunicati stampa, etc) ove non sia possibile identificare con precisione i singoli interessati coinvolti o non vi sia la disponibilità dei relativi dati di contatto ovvero si valuti che la comunicazione richieda sforzi sproporzionati.

- Sottopone al RL, per l'approvazione definitiva, sia il testo che le modalità per la comunicazione individuati in accordo con RPD.

Dell'avvenuta comunicazione è data informazione al RPD.

REGISTRAZIONE DELL'EVENTO – TENUTA DEL REGISTRO DEI DATA BREACH

Indipendentemente dalla notifica all'Autorità di controllo, il Titolare deve registrare e documentare qualunque violazione di dati personali (art. 33, par.5). Come ribadito dalle linee guida EDPB (Guidelines 01/2021), la tenuta del registro interno delle violazioni è un obbligo indipendente dal livello di rischio della violazione stessa e deve essere adempiuto in ogni caso.

Il Titolare istituisce, quindi, un Registro dei data breach, a disposizione del Garante della privacy, e da fornire all'occorrenza in caso di accertamenti da parte dell'Autorità (***All. 3***). La conservazione e l'aggiornamento del Registro sono affidati al Referente Interno Privacy. Nel Registro devono essere riportate:

- le informazioni necessarie a chiarire le circostanze nelle quali si sono verificate le violazioni;
- le conseguenze che le violazioni stesse hanno avuto;
- i provvedimenti adottati per porvi rimedio.

Nel Registro non devono essere riportati dati personali dei soggetti coinvolti nel data breach e nella gestione dello stesso.

Il Referente Interno Privacy dovrà aggiornare il Registro Data Breach contestualmente alla chiusura della fase di analisi, nel caso in cui risulti non necessaria la notifica al Garante Privacy o contestualmente all'invio di quest'ultima.

ATTIVITA' SUCCESSIVE

Se durante le fasi precedenti si sospetta che la violazione possa essere stata provocata in maniera intenzionale da un esterno o da un utente interno si attiva il processo di raccolta delle evidenze o prove con ulteriori investigazioni anche difensive.

L'attività, ove necessario, può essere gestita secondo quanto previsto dall'art. 391 *nonies*[1] o dall'art. 327 bis c.p.p.[2] e deve rispettare gli standard e le normative (raccolta e "catena di custodia") in termini di analisi forense, al fine di poter intraprendere successivamente un'azione legale nei confronti dell'eventuale responsabile.

Qualora non si riscontrasse questa condizione, l'analisi post-violazione sarà finalizzata all'apprendimento delle cause che hanno generato l'evento al fine di risolvere eventuali criticità collegate o ricorrenti.

Ad esito delle notificazioni al Garante ed agli interessati, il RPD deve:

- gestire in prima persona le relazioni e gli eventuali feedback pervenuti dal Garante e dalle altre Istituzioni coinvolte, coordinando – con l'ausilio della sua struttura di supporto – l'aggiornamento del "Registro dei Data Breach" (un cui modello è riportato nell'All. 3);
- gestire le comunicazioni, istanze e richieste da parte degli Interessati, anche attraverso un referente dell'attività di riferimento interessata dalla la violazione.

Qualora dalla violazione dei dati personali derivi un danno per gli interessati, sorge il tema della responsabilità del Titolare del trattamento ai sensi dell'articolo 82 del GDPR. È fondamentale comprendere che, secondo la consolidata giurisprudenza europea e nazionale, il diritto al risarcimento non è automatico. La Corte di Giustizia, nella Sentenza dell'11 aprile 2024 (Causa C-741/21), ha specificato che il risarcimento previsto dall'articolo 82 ha una funzione puramente compensativa e non punitiva. Pertanto, i criteri utilizzati per calcolare le sanzioni amministrative (articolo 83 GDPR) non sono applicabili per determinare l'importo del risarcimento del danno.

La Corte di Giustizia, nella Sentenza del 4 maggio 2023 (Causa C-300/21), e la giurisprudenza italiana, come il Tribunale di Ivrea con la Sentenza n.1265 del 21 Novembre 2024, hanno chiarito che il danno non è in re ipsa (cioè, implicito nella violazione stessa). L'interessato che agisce per il risarcimento deve dimostrare la sussistenza di tre elementi: 1) la violazione del GDPR; 2) di aver subito un danno (materiale o immateriale); 3) il nesso di causalità tra la violazione e il danno.

Il "danno immateriale" può includere la sofferenza e l'angoscia causate dalla violazione. La Corte di Giustizia, con la Sentenza del 14 dicembre 2023 (Causa C-340/21), ha stabilito che anche il semplice "timore di un potenziale utilizzo abusivo dei suoi dati personali" può costituire un danno immateriale risarcibile, a condizione che tale timore sia "fondato" nelle circostanze specifiche e non meramente ipotetico, come precisato nella Sentenza del 25 gennaio 2024 (Causa C-687/21).

È rilevante notare che, secondo la Sentenza della Corte di Giustizia del 26 settembre 2024 (Causa C-768/21), l'Autorità di controllo non è obbligata a imporre una sanzione amministrativa se la violazione è stata sanata dal titolare e un intervento correttivo non risulta appropriato, necessario o proporzionato. Questo valorizza l'importanza di una gestione diligente e tempestiva dell'incidente, come descritta in questa procedura.

FORMAZIONE

Nell'ambito del programma di formazione sulla sicurezza, nonché di quello permanente sulla tutela dei dati personali, L'Ordine svolge attività di informazione e formazione con riferimento ai contenuti del presente documento.

[1] Se precedente all'instaurazione di un procedimento penale.

[2] Se già instaurato il procedimento.

ALLEGATO 1 – MODELLO DI NOTIFICA AL GARANTE

Denominazione del Titolare del trattamento	
Dati di contatto	
Soggetto che effettua la notifica	
Ruolo del soggetto che effettua la notifica	
Responsabile della Protezione dei dati	
Dati di contatto del RPD	

Informazioni preliminari

Informazioni sulla notifica

☐ Nuova notifica
☐ Informazioni a completamento di una precedente notifica

Breve descrizione della violazione di dati personali

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

☐ Il _____
☐ Tra il _____ed il _____
☐ In un tempo non ancora determinato
☐ E' possibile che sia ancora in corso

Dove è avvenuta la violazione di dati?

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

Modalità di esposizione al rischio

Tipo di violazione

☐ 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 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)
☐ Altro:

Dispositivo oggetto della violazione

☐ Computer
☐ Dispositivo mobile
☐ Documento cartaceo
☐ File o parte di un file
☐ Strumento di back-up
☐ Rete
☐ Altro:

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione e del numero approssimativo di record registrati

Interessati colpiti dalla violazione di dati

☐ N. _____di persone fisiche
☐ Circa _____persone fisiche
☐ Un numero (ancora) sconosciuto di persone
☐ Descrizione della/e categoria/e di interessati coinvolti:

(per la categoria di interessati, ad es.: dipendenti dell'Ente, utenti del servizio….., etc.)

Tipologia di dati coinvolti nella violazione

☐ Dati anagrafici
☐ Numero di telefono (fisso o mobile)
☐ Indirizzo di posta elettronica
☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
☐ Altri dati di personali (sesso, data di nascita, età, ...), dati particolari, sanitari e giudiziari
☐ Ancora sconosciuto
☐ Altro:

Livello di gravità della violazione dei dati personali e possibili conseguenze

(secondo le valutazioni del Titolare)

Contromisure (azioni preventive e correttive)

Misure tecniche e organizzative applicate prima della violazione

Misure tecniche e organizzative applicate successivamente alla violazione per attenuarne le conseguenze

Comunicazione agli interessati

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il _____

☐ No, perché:

Contenuto della comunicazione agli interessati

Canale utilizzato per la comunicazione agli interessati

ALLEGATO 2 – MODELLO DI COMUNICAZIONE ALL'INTERESSATO (*)

Denominazione del Titolare del trattamento	
Dati di contatto	
Soggetto che effettua la notifica	
Ruolo del soggetto che effettua la notifica	
Responsabile della Protezione dei dati	
Dati di contatto del RPD	

Interessato destinatario della comunicazione	

Modalità della comunicazione

☐ Raccomandata A/R
☐ PEC
☐ Posta elettronica
☐ Fax
☐ Altro: _____

Spett. Società/Egr. Sig……./

siamo spiacenti di informare che in data ..... abbiamo rilevato di aver subito una violazione dei dati personali la riguardano.

Nel prosieguo, in termini sintetici, è fornito – ai sensi di quanto previsto dall'art. 34 Regolamento UE n. 679/2016 (GDPR) – un quadro di quanto è accaduto.

La violazione è stata anche notificata al Garante.

Breve descrizione della violazione di dati personali e delle sue modalità

(*) Qualora la comunicazione richieda – ex art. 34, par. 3, lett. c) del GDPR – uno sforzo proporzionato (in relazione, per es. alle attività da svolgere e/o ai costi da sostenere), "(…) si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia".

Dispositivo oggetto della violazione

☐ Computer
☐ Dispositivo mobile
☐ Documento cartaceo
☐ File o parte di un file
☐ Strumento di back-up
☐ Rete
☐ Altro:

Tipologia di dati coinvolti nella violazione

☐ Dati anagrafici
☐ Numero di telefono (fisso o mobile)
☐ Indirizzo di posta elettronica
☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
☐ Altri dati di personali (sesso, data di nascita, età, ...), dati particolari, sanitari e giudiziari
☐ Ancora sconosciuto
☐ Altro:

Tipo di violazione

☐ 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 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)
☐ Altro:

Livello di gravità della violazione dei dati personali e possibili conseguenze

Indicare:
A) Numero approssimativo di registrazioni dei dati personali oggetto della violazione
B) Categoria e numero approssimativo degli interessati coinvolti dalla violazione
C) Livello di gravità elevato della violazione per i diritti e le libertà delle persone fisiche
D) Possibili conseguenze della violazione.

(secondo le valutazioni del Titolare)

Misure tecniche e organizzative applicate preventivamente e quelle applicate successivamente alla violazione per porre rimedio alla violazione o per attenuarne le conseguenze

Per ulteriori informazioni, può essere contattato …….

ALLEGATO 3 – REGISTRO DEI DATA BREACH

DETTAGLI DELLA VIOLAZIONE					CONSEGUENZE DELLA VIOLAZIONE		AZIONI CORRETTIVE		NOTIFICHE / COMUNICAZIONI		
Data evento e data conoscenza	Attività interessata dall'evento	Natura dell'evento e breve descrizione della violazione	Tipologie di dati interessati	Categorie interessati coinvolti	Effetti accertati	Effetti ipotizzabili / possibili	Azioni correttive implementate	Azioni correttive da intraprendere	Notifica Garante	Comunicazione interessati	Doc. / allegati e/o email