Procedura di Gestione delle Violazioni dei dati personali in attuazione del Regolamento (UE) 2016/679

INDICE

1. Contenuto e scopo

La presente Procedura prescrive le modalità con cui sono gestite e documentate nell'Ente le violazioni dei dati personali, ai sensi degli articoli 33 e 34 del Regolamento (UE) 2016/679 ("GDPR") e del D. Lgs. 196/2003 ("Codice").

2. Definizioni

Nella presente Procedura si fa riferimento alle seguenti definizioni:

Titolare: ai sensi dell'art.4.7 GDPR, il Titolare del trattamento ("Titolare") coincide con la persona giuridica dell'Ente.

Responsabile di Unità (RdU): ogni persona fisica designata dal Titolare come responsabile dell'attuazione della protezione dei dati personali nell'ambito di una unità organizzativa dell'Ente, ai sensi dell'art 4.8 GDPR (Responsabile interno del trattamento) o dell'art. 2-quaterdecies comma 1 del Codice ("Soggetto Designato"). Nell'organizzazione dell'ente coincide con la figura organizzativa apicale dell'unità stessa.

Responsabile Privacy: figura designata dal Titolare a valutare le violazioni riconducibile al dirigente della Struttura cui sono ricondotte le funzioni in materia di Privacy. Nell'organizzazione dell'ente è il dirigente dell'Ufficio di Staff Personale, Affari generali e contratti.

Referente Privacy: figura designata a mantenere i rapporti con RPD ed a coordinare operativamente le attività di protezione dei dati personali nell'Ente,

Referente CED: figura che coadiuva operativamente il Referente Privacy nelle attività di protezione dei dati personali nell'Ente.

Incaricato: ai sensi dell'art.29 GDPR e dell'art. 2-quaterdecies comma 2 Codice, ogni dipendente o collaboratore autorizzato dal Titolare o dal proprio RdU a trattare dati personali nell'ambito dell'unità organizzativa di assegnazione.

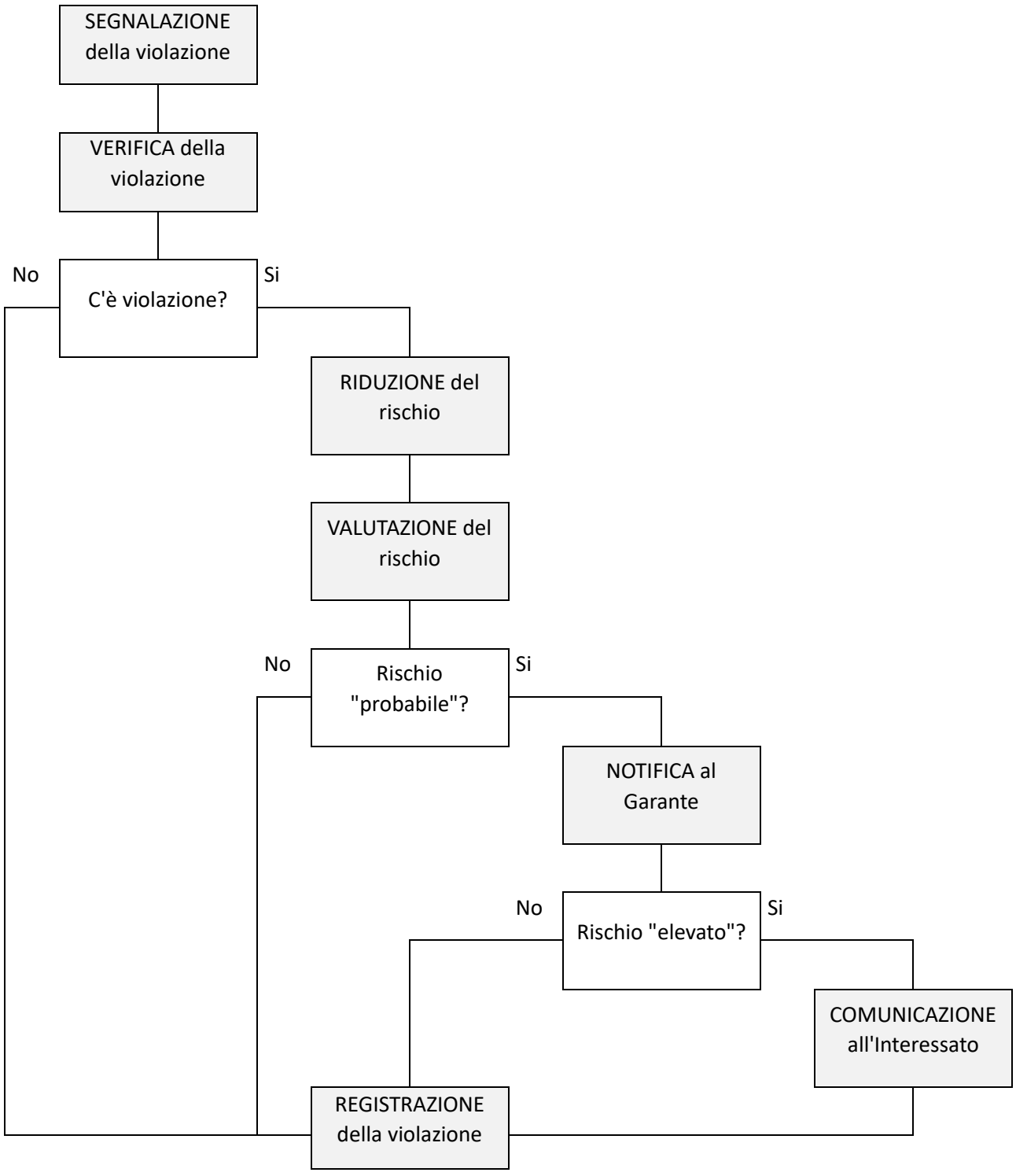
Responsabile esterno: ai sensi dell'art.28 GDPR, ogni fornitore di servizi che tratta dati personali per conto del Titolare sulla base di un contratto o altro atto giuridico equivalente stipulato tra Titolare e Responsabile esterno.

Amministratore di Sistema (AdS): figura responsabile della gestione dei sistemi informativi su cui sono trattati dati personali (cfr. "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 - G.U. n. 300 del 24 dicembre 2008")

Responsabile per la Protezione dei Dati (RPD): figura designata dal Titolare ai sensi degli art.37-38-39 GDPR con compiti di sorveglianza e consulenza.

3. Fasi della gestione delle violazioni

Ai sensi degli artt. 33 e 34 GDPR, le violazioni sono gestire secondo le seguenti fasi:



Nel seguito del presente documento sono descritte le attività previste in ogni fase e le corrispondenti responsabilità all'interno dell'Ente.

4. Segnalazione della violazione

Le segnalazioni di potenziali violazioni possono pervenire dall'interno dell'ente, dall'esterno o essere automatiche generate dai sistemi informatici.

Segnalazioni interne

Ogni Incaricato è tenuto a segnalare tempestivamente al proprio RdU ogni situazione di cui è venuto a conoscenza che può comportare una violazione di dati personali.

La segnalazione è effettuata preferibilmente per iscritto inoltrando apposita comunicazione a mezzo mail all'indirizzo istituzionale del RdU

La segnalazione contiene le seguenti informazioni, utili alla successiva fase di Verifica:

- La **categoria di dati personali** (es. dati identificativi, residenza, dati sanitari, dati giudiziari, dati biometrici…)
- La **categoria degli Interessati** (es. clienti, cittadini, fornitori, dipendenti, amministratori, minori, utenti o beneficiari di specifici servizi …)
- la **quantità di Interessati** (es. uno, pochi, tutti)
- **come e quando** si è venuti a conoscenza della situazione
- quale **ruolo** ha avuto il segnalatore nella situazione (es. è in copia di una mail, è il mittente della mail …)
- eventuali **azioni già intraprese** in risposta alla situazione

È fatto divieto agli Incaricati di diffondere - nell'ente o fuori dall'ente - informazioni relative alle situazioni segnalate.

Ai sensi del'art.29 GDPR, il Titolare attraverso l'Ufficio Personale-predispone e distribuisce la presente procedura per la segnalazione delle potenziali violazioni, inviandola a mezzo mail e protocollo ai singoli RdU affinché questi ne curino e verifichino la trasmissione ai singoli incaricati

Segnalazioni esterne

Con le medesime modalità delle segnalazioni interne, gli Incaricati trasmettono anche le segnalazioni proveniente dall'esterno dell'Ente e di cui siano venuti a conoscenza da mail, telefonata, media, social network ecc.

Segnalazioni automatiche

Gli AdS predispongono e monitorano sistemi digitali (es. antivirus, antiramsomware, IDS/IPS) in grado di intercettare e segnalare automaticamente potenziali violazioni di dati personali.

Gli AdS sottopongono tempestivamente al Responsabile Privacy le potenziali violazioni e curano la reportistica periodica relativa alle segnalazioni automatiche, a supporto della valutazione complessiva dell'efficacia della protezione "fin dalla progettazione e per impostazione predefinita" (art. 25 GDPR).

5. Verifica della violazione

Ricevuta la segnalazione, il Responsabile Privacy avvia la Verifica della potenziale violazione, coinvolgendo: il RdU da cui proviene o in cui potrebbe essere avvenuta la violazione medesima, il Referente Privacy, il referente CED, gli AdS ed i Responsabili esterni convolti e anche il RPD.

La Verifica ha lo scopo di appurare se sia realmente avvenuta una violazione:

- Se la Verifica **conferma la violazione** di dati personali, vengono subito avviate le prime misure tecnico – organizzative utili a contenere il rischio per gli interessati. A fini dell'art.33.1 GDPR, da questo momento il Titolare è da ritenersi "a conoscenza" della violazione e conseguentemente partono le 72 ore entro cui provvedere alla notifica al Garante, se necessario.
- Se invece la Verifica **esclude la violazione** di dati personali, il RdU procede alla chiusura del caso.

In entrambi i casi, la segnalazione viene registrata a cura del Referente Privacy coadiuvato dal referente CED nel Registro delle Violazioni, salvo per le segnalazioni manifestatamente non fondate.

6. Riduzione del rischio

Acclarata la violazione, il Responsabile Privacy coordina le prime misure tecniche ed organizzative in grado di ridurre il rischio per i diritti e le libertà degli interessati, in ottemperanza dell'art.34.3.c GDPR: "*il titolare [adotta] misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati*".

Esempi di misure atte a ridurre il rischio sono il blocco o reset degli account violati da un furto di password, il recupero da backup di dati bloccati da un ramsomware, l'oscuramento dal sito istituzionale di dati erroneamente pubblicati, l'invio di una mail di rettifica ecc.

Le misure attuate sono sinteticamente riportate nel Registro delle Violazioni.

7. Valutazione del rischio

Acclarata la violazione, la Valutazione del rischio ha lo scopo di valutare il **livello del rischio** per i diritti e le libertà degli Interessati comportato dalla medesima.

Con riferimento all'art.33.1 GDPR:

"In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo ... a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche."

La Valutazione deve distinguere tra rischio "**probabile**" (che richiede la notifica al Garante) ed "**improbabile**" (che non la richiede).

Se il rischio è "probabile", con riferimento all'art.34.1 GDPR:

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

la Valutazione deve verificare se il rischio è **"elevato**", livello che richiede anche la Comunicazione agli interessati.

Per la Valutazione del rischio, occorre tener conto sia del potenziale **danno** causato agli interessati dalla violazione sia della **probabilità** che il danno occorra realmente.

La valutazione del danno dipende dalla categoria di dati personali violati (es. la violazione di dati sanitari comporta un danno più elevato rispetto alla violazione dei dati identificativi), dalla categoria di interessati coinvolti (es. una violazione relativa ai dati di un minore comporta normalmente un danno superiore alla violazione di dati di un adulto) e dalla loro numerosità.

La valutazione della probabilità dipende dalle misure tecniche ed organizzative messe in campo per proteggere i dati sia prima della violazione (es. lo smarrimento di un portatile comporta una probabilità trascurabile di violazione - e quindi un rischio minimo- se i dati in esso memorizzati erano stati crittografati) sia dopo (cfr. Riduzione del rischio).

La Valutazione è svolta dal Responsabile Privacy e si conclude con la definizione del livello del rischio:

Rischio	Notifica al Garante	Comunicazione all'Interessato	Registrazione nel Registro Violazioni
Improbabile	NO	NO	SI
Probabile	SI	NO	SI
Elevato	SI	SI	SI

La Valutazione è sinteticamente riportata nel Registro delle Violazioni.

8. Notifica al Garante

Se il rischio per l'Interessato è valutato "probabile" o "elevato", il Referente Privacy coadiuvato dal referente CED predispone la Notifica al Garante, la sottopone alla firma del legale rappresentante del Titolare (o ad altra figura delegata allo scopo dal legale rappresentante) e la invia al Garante attraverso l'apposito sistema on line.

Il sistema del Garante assegna alla Notifica un codice identificativo univoco.

La Notifica deve essere inviata al Garante entro le 72 ore dal momento in cui la Verifica ha confermato la violazione. Per rispettare questo vincolo temporale in caso di informazioni incomplete, si può procedere ad una Notifica "preliminare", cui seguirà una Notifica di chiusura appena si disporrà delle informazioni mancanti. Per il corretto collegamento tra le due Notifiche, è necessario citare nella Notifica di chiusura il codice identificativo della Notifica preliminare.

Il Referente Privacy coadiuvato dal referente CED invia a RPD copia della Notifica e lo tiene informato relativamente alle eventuali successive comunicazioni da parte del Garante.

9. Comunicazione all'Interessato

Se il rischio per l'Interessato è valutato "elevato", il Responsabile Privacy predispone una comunicazione agli Interessati che descrive (art. 34.2 GDPR) *"con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d)"* e cioè i contatti del RPD e del Titolare presso cui chiedere più informazioni, le probabili conseguenze della violazione dei dati personali e le misure di riduzione del rischio adottate o che si intende adottare.

Non è richiesta la Comunicazione all'Interessato se è soddisfatta una delle condizioni di cui all'art. 34.3.

10.Registrazione della violazione

Con riferimento all'art. 34.5 GDPR:

"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".

E' istituito nell'Ente il "Registro delle Violazioni" in cui vengono registrate le Segnalazioni verificate, indipendentemente dall'esito della Valutazione, salvo le Segnalazioni manifestatamente non fondate.

Il Registro delle Violazioni viene custodito nel rispetto della normativa vigente in materia.

11.Monitoraggio periodico

Il Responsabile Privacy verifica annualmente l'applicazione della presente Procedura, riportando al Titolare l'esito della verifica attraverso un Rapporto contenente almeno le seguenti informazioni ed il loro andamento nel tempo (tra parentesi il valore ottimale cui tendere):

- Numero Segnalazioni dall'esterno / totale Segnalazioni (0%)
- Numero Segnalazioni automatiche / totale Segnalazioni (100%)
- Numero di Violazioni nell'anno per unità organizzativa dell'Ente (0%)
- Numero di Notifiche / Numero di Violazioni nell'anno (0%)
- Numero di Notifiche / Numero di Comunicazioni nell'anno (0%)
- Giorni medi trascorsi tra violazione e sua "conoscenza" da parte dell'Ente (0)