PROVINCIA di VARESE

DELIBERAZIONE DEL PRESIDENTE

N. 90 DEL 25/06/2026

OGGETTO: APPROVAZIONE DELLA PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH) E DEL MODELLO DI REGISTRO DELLE VIOLAZIONI

L'anno **2026**, addì **25** del mese di **giugno** alle ore **16:43,** nella sala delle adunanze del palazzo provinciale il Presidente MARCO MAGRINI con la partecipazione del Segretario Generale STEFANEA LAURA MARTINA adotta il seguente provvedimento:

PROVINCIA di VARESE

IL PRESIDENTE

Con i poteri conferiti dalla Legge n. 56/2014 che disciplina le competenze dello stesso "… rappresenta l'Ente, convoca e presiede il Consiglio Provinciale e l'Assemblea dei Sindaci, sovrintende al funzionamento dei servizi e degli uffici e all'esecuzione degli atti; esercita le altre funzioni attribuite dallo Statuto"

Visto lo statuto della Provincia di Varese adottato dal Consiglio Provinciale nella seduta del 30 luglio 2019 con deliberazione n. 29 ed in particolare l'art. 14 "Elezione e competenze " e l'art. 15 "Atti Presidenziali";

Premesso che:

- Il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»* (di seguito *RGPD*), in vigore dal 24 maggio 2016, e applicabile dal 25 maggio 2018, prevede che tutti i titolari del trattamento sono tenuti ad osservare una serie di obblighi per garantire la sicurezza dei dati trattati;

- il sopracitato Regolamento pone con forza l'accento sulla "responsabilizzazione" di titolari e responsabili, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento;

Considerato che:

- l'art. 33 del Regolamento prevede che tutti i titolari dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque senza ingiustificato ritardo, se ritengono probabile che da tale violazione derivino dei rischi per i diritti e le libertà degli interessati;

- l'art. 34 del Regolamento prevede che se la probabilità di tale rischio è elevata si dovrà informare della violazione anche gli interessati, sempre senza ingiustificato ritardo;

Rilevato che:

- la notifica all'Autorità dell'avvenuta violazione è obbligatoria solo sotto particolari circostanze, subordinata alla valutazione del rischio per gli interessati;

- il Titolare dovrà comunque documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati nonché le relative circostanze e conseguenze e i provvedimenti adottati, essendo peraltro tenuto a fornire tale documentazione su richiesta all'autorità di controllo in caso di accertamenti:

Valutato che:

- occorre disciplinare gli aspetti organizzativi e la procedura che definisca le modalità operative, i compiti e le responsabilità relative alla gestione delle violazioni di dati personali che potrebbero comportare un rischio per i diritti e le libertà delle persone fisiche;

- il personale incaricato dall'ente, in collaborazione con il Responsabile della Protezione dei Dati, ha redatto un una procedura in cui sono definite le modalità operative, i compiti e le responsabilità relative alla gestione delle violazioni di dati personali, cui è allegato quale parte integrante e sostanziale lo Schema di Registro delle Violazioni di dati personali;

Ritenuto di dover approvare la procedura sopra menzionata e dato atto della necessità di individuare dei soggetti referenti che ricevano e gestiscano tutte le segnalazioni di incidente relative all'ente;

Visti i seguenti pareri espressi ai sensi dell'art. 49, comma 1 del D.Lgs. 267/18.08.2000:

- parere "favorevole" in ordine alla regolarità tecnica espresso dal Dirigente dell'Area Presidenza, Segreteria e Direzione Generale, Dott.ssa Stefanea Laura Martina;

- parere favorevole in ordine alla regolarità contabile espresso dal Dirigente dell'Area Risorse, Dott. Raffaele Buononato

DELIBERA

1) di approvare la Procedura per la gestione delle violazioni di dati personali (cd. Data Breach) nonché l'allegato Schema di Registro delle Violazioni di dati personali;

2) di nominare con separato decreto le figure individuate nella procedura di Data Breach con il compito di assistere e coadiuvare il Titolare nella rilevazione, valutazione ed eventuale segnalazione all'Autorità di Controllo delle violazioni di dati;

3) di dare notizia dell'adozione del presente atto ai Dirigenti ed ai Titolari di EQ perché prendano consapevolezza dei comportamenti da tenere e collaborino per la gestione degli eventuali incidenti di sicurezza occorsi nelle unità organizzative di propria competenza, nel rispetto della procedura adottata;

4) di pubblicare la presente deliberazione di approvazione della Procedura di Gestione delle Violazioni dei dati personali in attuazione del Regolamento (UE) 2016/679, nella Sezione Amministrazione Trasparente dell'Ente;

5) di dare atto che il presente provvedimento non comporta l'assunzione di alcun onere finanziario;

6) di dare atto che sul presente provvedimento sono stati espressi favorevolmente i pareri ai sensi dell'art. 49, comma 1 del D.Lgs. 267/18.08.2000;

7) di dare atto, altresì, che tale provvedimento emanato da organo monocratico rappresenta una decisione derivante da valutazioni tecniche e pertanto segue l'iter procedimentale e consequenziale a quello già fissato per le deliberazioni dell'organo esecutivo;

8) di dichiarare il presente provvedimento immediatamente eseguibile, ai sensi dell'art. 134, comma 4, D.Lgs. 267/18.08.2000, stante la necessità di adottare tempestivamente la procedura in oggetto per adempiere all'adeguamento normativo richiesto dal Regolamento UE 679/2016 e per rispettare il cronoprogramma concordato con il DPO dell'Ente.

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.

IL PRESIDENTE
MARCO MAGRINI

IL SEGRETARIO GENERALE
STEFANEA LAURA MARTINA

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.

Soggetto Designato: ai sensi dell'art. 2-quaterdecies comma 1 del Codice, ogni persona fisica designata dal Titolare come responsabile dell'attuazione della protezione dei dati personali nell'ambito di una unità organizzativa dell'Ente (Settore); per la Provincia di Varese il ruolo di Soggetto Designato è svolto dai **Responsabili di Settore**, titolari di incarico di Elevata Qualificazione.

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

Responsabile Privacy: figura designata dal Titolare a valutare le violazioni; per Provincia di Varese il ruolo è svolto dal **Dirigente dell'Area Presidenza, Segreteria e Direzione Generale**.

Referente Privacy: figura designata dal Titolare a mantenere i rapporti con RPD ed a coordinare operativamente le attività di protezione dei dati personali nell'Ente; per Provincia di Varese il ruolo è svolto dal **Settore Organizzazione e Segreteria.**

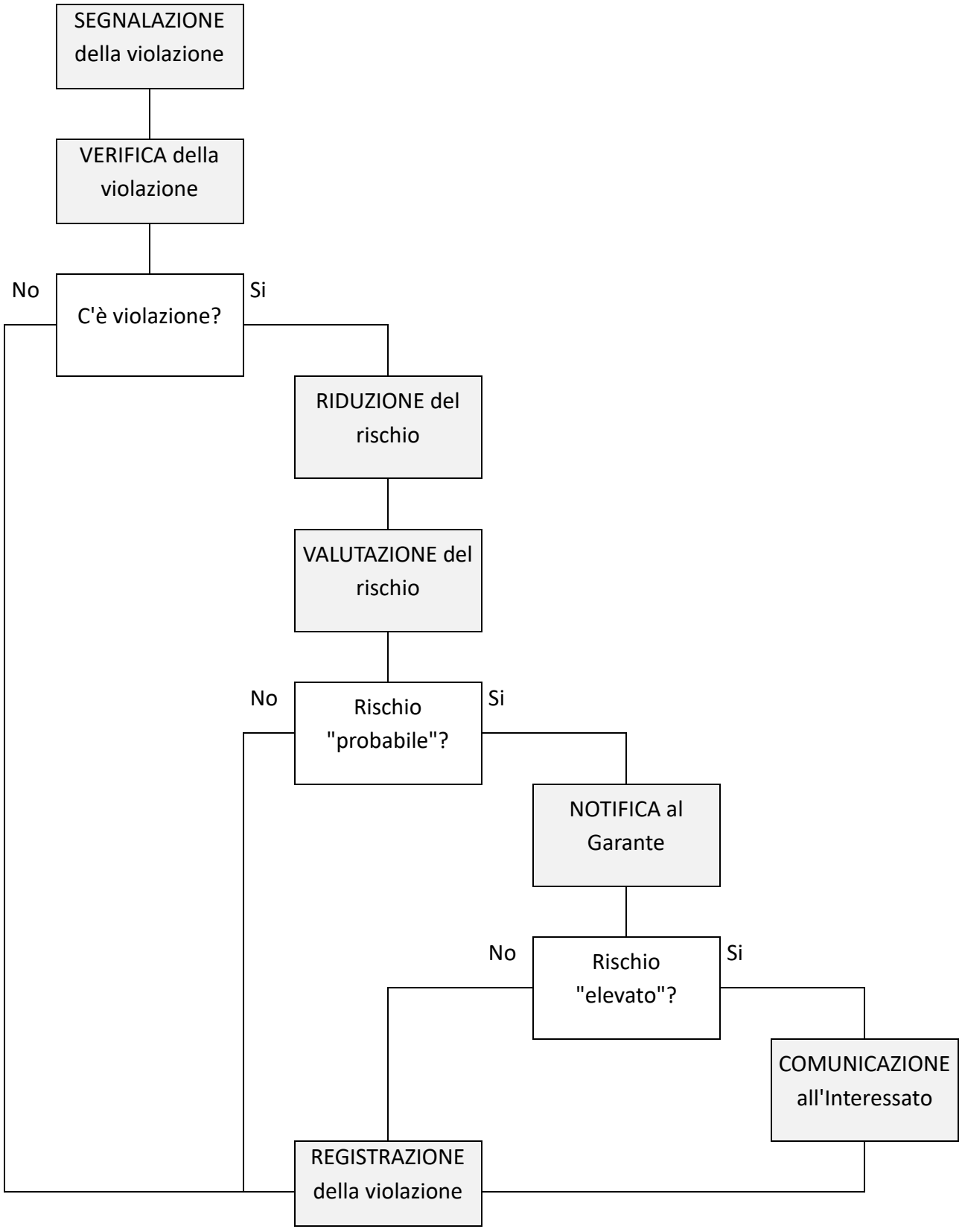
Responsabile esterno: ai sensi dell'art. 28 GDPR, ogni fornitore di servizi che tratta dati personali per conto del Titolare sulla base di un contratto o altro atto giuridico equivalente stipulato tra Titolare e Responsabile esterno.

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 **Autorizzato** è tenuto a segnalare tempestivamente al proprio **Responsabile di Settore (Soggetto Designato)**, al **Responsabile Privacy** (**Dirigente dell'Area Presidenza**) e al **Referente Privacy** (**Settore Organizzazione e Segreteria**) ogni situazione di cui è venuto a conoscenza che può comportare una violazione di dati personali.

La segnalazione è effettuata preferibilmente per iscritto scrivendo una mail agli indirizzi istituzionali indirizzata al Responsabile di Settore, al Responsabile Privacy (Dirigente Area Presidenza) e al Referente Privacy (Settore Organizzazione e Segreteria).

La segnalazione dovrebbe 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 (es. ha chiamato il mittente della mail, ha distrutto una copia di un documento riservato lasciata alla macchina del caffè)

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

Ai sensi dell'art. 29 GDPR, il Titolare attraverso il Responsabile Privacy e/o Referente Privacy divulga la presente, inviandola a mezzo mail ai Responsabili di Settore, affinché questi ne curino e verifichino la trasmissione ai singoli Autorizzati.

Segnalazioni esterne

Con le medesime modalità delle segnalazioni interne, gli Autorizzati 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** (Dirigente Area Presidenza) 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** (Dirigente Area Presidenza) avvia la Verifica della potenziale violazione, coinvolgendo il **Responsabile di Settore** da cui proviene la segnalazione o in cui potrebbe essere avvenuta la violazione, il Referente Privacy, gli AdS ed i Responsabili esterni convolti e, nei casi più complessi, anche il RPD.

La Verifica ha lo scopo di verificare 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 **Responsabile di Settore** procede alla chiusura del caso (previa registrazione nel Registro delle Violazioni).

In entrambi i casi, la segnalazione viene registrata a cura del Responsabile Privacy e/o Referente Privacy nel Registro delle Violazioni, salvo per le segnalazioni manifestatamente non fondate.

6. Riduzione del rischio

Acclarata la violazione, il **Responsabile Privacy** (Dirigente Area Presidenza) 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 – che viene svolta dal **Responsabile Privacy** (Dirigente Area Presidenza) con il supporto del **Referente Privacy** (Settore Organizzazione e Segreteria) ed eventualmente del **RPD** - ha lo scopo di valutare il **livello del rischio** per i diritti e le libertà degli Interessati comportato dalla violazione.

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. paragrafo 6 - Riduzione del rischio).

La Valutazione 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 a cura del **Responsabile Privacy** (Dirigente Area Presidenza) con il supporto del **Referente Privacy** (Settore Organizzazione e Segreteria).

8. Notifica al Garante

Se il rischio per l'Interessato è valutato "probabile" o "elevato", il **Responsabile Privacy** e/o il **Referente Privacy** predispone la Notifica al Garante, la sottopone alla firma del Titolare (o ad altra figura delegata allo scopo) 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 **Responsabile Privacy** e/o il **Referente Privacy** invia al 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 in collaborazione con il **Referente Privacy** 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".

È istituito nell'Ente il "**Registro delle Violazioni**", allegato alla presente procedura, in cui vengono registrate le Segnalazioni verificate, indipendentemente dall'esito della Valutazione, salvo le Segnalazioni manifestatamente non fondate.

Il **Responsabile Privacy** in collaborazione con il **Referente Privacy** cura la compilazione e custodisce il Registro delle Violazioni.

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)

Provincia di Varese

Registro delle Violazioni

Il Registro è formato da un Indice delle Registrazioni e da una Scheda di dettaglio per ogni Registrazione. Compilare una riga dell'Indice per ogni Scheda. Allegare alle Schede copia delle eventuali Notifiche e Comunicazioni.

INDICE DELLE REGISTRAZIONI

N.	Data	Descrizione breve dell'evento	Codice Notifica	Comunicazione (Si/No)
1				
2				
3				

SCHEDA N. XXXX	
VERIFICA DELLA VIOLAZIONE	
Data e ora	Data e ora termine analisi della Segnalazione, da cui partono le 72 ore
Descrizione	Sintesi della Segnalazione: chi ha segnalato cosa, quando e come
Avvenuta Violazione?	No | Si
Data della violazione	Data presunta della violazione
Descrizione violazione	Descrizione sintetica dei fatti
Tipo violazione	Riservatezza, Integrità, Disponibilità
Dati personali violati	Es. dati identificativi, sanitari, giudiziari …
Interessati coinvolti	Es. cittadini, utenti di un servizio, minori, fornitori, dipendenti…
Quantità Interessati	Stima del numero di Interessati coinvolti
Sistemi Informativi	Es. Anagrafe, Contabilità, Protocollo, cartelle condivise, posta elettronica
Archivi cartacei	Es. Archivio Edilizia Privata, Fascicoli del Personale
Sedi e unità coinvolte	Es. sede principale, magazzino; Ufficio Tributi
Analisi di	Nome e ruolo di chi ha la responsabilità dell'analisi
VALUTAZIONE DEL RISCHIO	
Livello rischio	Improbabile | Probabile | Elevato
Motivazione	Sintesi delle motivazioni che portano al livello di rischio
Misure di riduzione	Misure di riduzione del rischio attuate nell'immediato
Misure successive	Misure di riduzione del rischio successivamente adottate o pianificate
Valutazione di	Nome e ruolo di chi ha la responsabilità della valutazione
NOTIFICA AL GARANTE (solo se Rischio = probabile o elevato)	
Data e ora Notifica	Data ed ora invio Notifica
Firmata da	Nome e ruolo di chi l'ha firmata
Codice Garante	Codice identificativo rilasciato dal Garante
Notifica di chiusura	Data e ora di invio Notifica di chiusura
COMUNICAZIONE AGLI INTERESSATI (solo se Rischio = elevato)	
Data avvio	Data di avvio delle comunicazioni agli interessati
Modalità	Es. lettera al domicilio, mail, avviso sul sito istituzionale

PROVINCIA di VARESE

SETTORE ORGANIZZAZIONE E SEGRETERIA

PARERE DI REGOLARITA' TECNICA

Vista la proposta di deliberazione n. 2942/2026 con oggetto:APPROVAZIONE DELLA PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH) E DEL MODELLO DI REGISTRO DELLE VIOLAZIONI si esprime parere FAVOREVOLE in ordine alla regolarità tecnica ai sensi dell'art. 49, comma 1 del D.L.vo 18 Agosto 2000, n. 267

Varese, 24/06/2026

IL DIRIGENTE
STEFANEA LAURA MARTINA

(Sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

PROVINCIA di VARESE

SETTORE FINANZE E BILANCIO

PARERE DI REGOLARITA' CONTABILE

Vista la proposta di deliberazione n. 2942/2026 con oggetto: APPROVAZIONE DELLA PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH) E DEL MODELLO DI REGISTRO DELLE VIOLAZIONI si esprime parere FAVOREVOLE in ordine alla regolarità contabile ai sensi dell'art. 49, comma 1 del D.L.vo 18 Agosto 2000, n. 267

Varese, 25/06/2026

IL DIRIGENTE
RAFFAELE BUONONATO

(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)