PROVINCIA DI PIACENZA

Provv. N. 41 del 25/03/2024

Proposta n. 435/2024

OGGETTO: REGOLAMENTO UE 2016/679 GENERAL DATA PROTECTION REGULATION (GDPR) - APPROVAZIONE DELLA PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI

IL PRESIDENTE

Considerato che il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (abrogativo della vigente direttiva 95/46 CE) ha introdotto un nuovo quadro giuridico nella materia della protezione dati personali applicabile dal 25 maggio 2018 ai sensi di quanto disposto dall'Art. 99, paragrafo 2 del Regolamento (UE) 2016/679;

Atteso che le principali novità introdotte dal Regolamento (UE) 2016/679 sono da collegarsi sostanzialmente alla centralità dei principi di adeguatezza e responsabilizzazione, intesi come "adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento" (così il Garante per la Protezione dei Dati personali nella sua Guida all'applicazione del Regolamento europeo);

Dato atto che il suddetto Regolamento introduce l'obbligo di notificare all'autorità di controllo nazionale (Garante Privacy) incidenti sulla sicurezza che comportino la violazione dei dati personali *(data breach)* e di rendere nota la violazione stessa alle persone fisiche interessate;

Rilevato che gli artt. 33 e 34 del Regolamento (UE) 2016/679 ("GDPR") e del D. Lgs. 196/2003 ("Codice") disciplinano la gestione delle violazioni dei dati personali prescrivendo specificatamente che:

Art.33:

- Comma 1" *In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".*
- Comma 2. "*Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione*".

  ……
- Comma 5. "*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".*

Art.34:

- Comma 1. "*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".*

  ……

Dato atto che, ai sensi dei sopra citati articoli, la notifica all'autorità di controllo deve obbligatoriamente contenere almeno i seguenti elementi:

- descrizione della natura della violazione dei dati personali e le registrazioni dei dati personali in questione;
- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere maggiori informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o da adottare 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.

Tenuto presente che la violazione dei dati personali è da intendersi come la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati tale da impedire al titolare del trattamento di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del GDPR.;

Considerato che l'ente si è già dotato di un registro interno di violazioni, dove vengono annotate sia le violazioni non notificabili che quelle notificabili, contenente i seguenti dati:

- i dettagli relativi alla violazione (cause, fatti e dati personali interessati);
- gli effetti e le conseguenze della violazione;

- i provvedimenti adottati per porvi rimedio;
- il ragionamento alla base delle decisioni prese in risposta a una violazione (con particolare riferimento alle violazioni non notificate ed alle violazioni notificate con ritardo).

Rilevato che, per quanto sopra esposto, è necessario ora istituire ed approvare una Procedura di gestione delle violazioni avente lo scopo di indicare le modalità di gestione del *data breach;*

Dato atto che al fine di garantire la massima diffusione interna ed esterna e la massima conoscibilità sulle azioni da intraprendere e sui comportamenti da adottare in caso di *data breach*, l'Ente è tenuto a garantire la pubblicazione della Procedura delle violazioni sul sito web istituzionale nella sezione "Privacy", nonché a garantire la conoscibilità della stessa a tutti i dipendenti dell'Ente;

Considerato che:

- L'Ente ha provveduto a redigere il documento che contiene la Procedura di Gestione delle Violazioni dei dati personali in attuazione del Regolamento (UE) 2016/679 (Allegato A);
- Il suddetto documento è stato validato dal Responsabile della Protezione dei dati (DPO);

Preso atto che è necessario procedere a dichiarare immediatamente eseguibile la presente deliberazione per adempiere tempestivamente all'adeguamento normativo GDPR 679/2016;

Visti:

-il Testo Unico degli Enti Locali;

-il vigente Statuto dell'Ente;

-il Regolamento di organizzazione degli uffici e dei servizi;

Acquisito il parere favorevole, espresso in merito alla regolarità tecnica dell'assumenda proposta, sottoscritto dal Dirigente dell'Ufficio di Staff Personale, Affari Generali, Contratti reso ai sensi dell'art. 49 del Testo Unico degli Enti Locali approvato con D.Lgs. 18/8/2000 n° 267;

DISPONE

1. **Di approvare**, per i motivi esposti in premessa e che qui si intendono integralmente riportati e trascritti, la Procedura di Gestione delle Violazioni dei dati personali in attuazione del Regolamento (UE) 2016/679, di cui all'allegato A;
2. **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;

3. **di dare atto che** il presente provvedimento non comporta l'assunzione di alcun onere finanziario ed è esecutivo alla data della sua sottoscrizione.

IL PRESIDENTE DELLA PROVINCIA

PATELLI MONICA

con firma digitale

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

INDICE

1. CONTENUTO E SCOPO 3
2. DEFINIZIONI 3
3. FASI DELLA GESTIONE DELLE VIOLAZIONI 4
4. SEGNALAZIONE DELLA VIOLAZIONE 5
5. VERIFICA DELLA VIOLAZIONE 6
6. RIDUZIONE DEL RISCHIO 6
7. VALUTAZIONE DEL RISCHIO 6
8. NOTIFICA AL GARANTE 7
9. COMUNICAZIONE ALL'INTERESSATO 7
10. REGISTRAZIONE DELLA VIOLAZIONE 8
11. MONITORAGGIO PERIODICO 8

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.

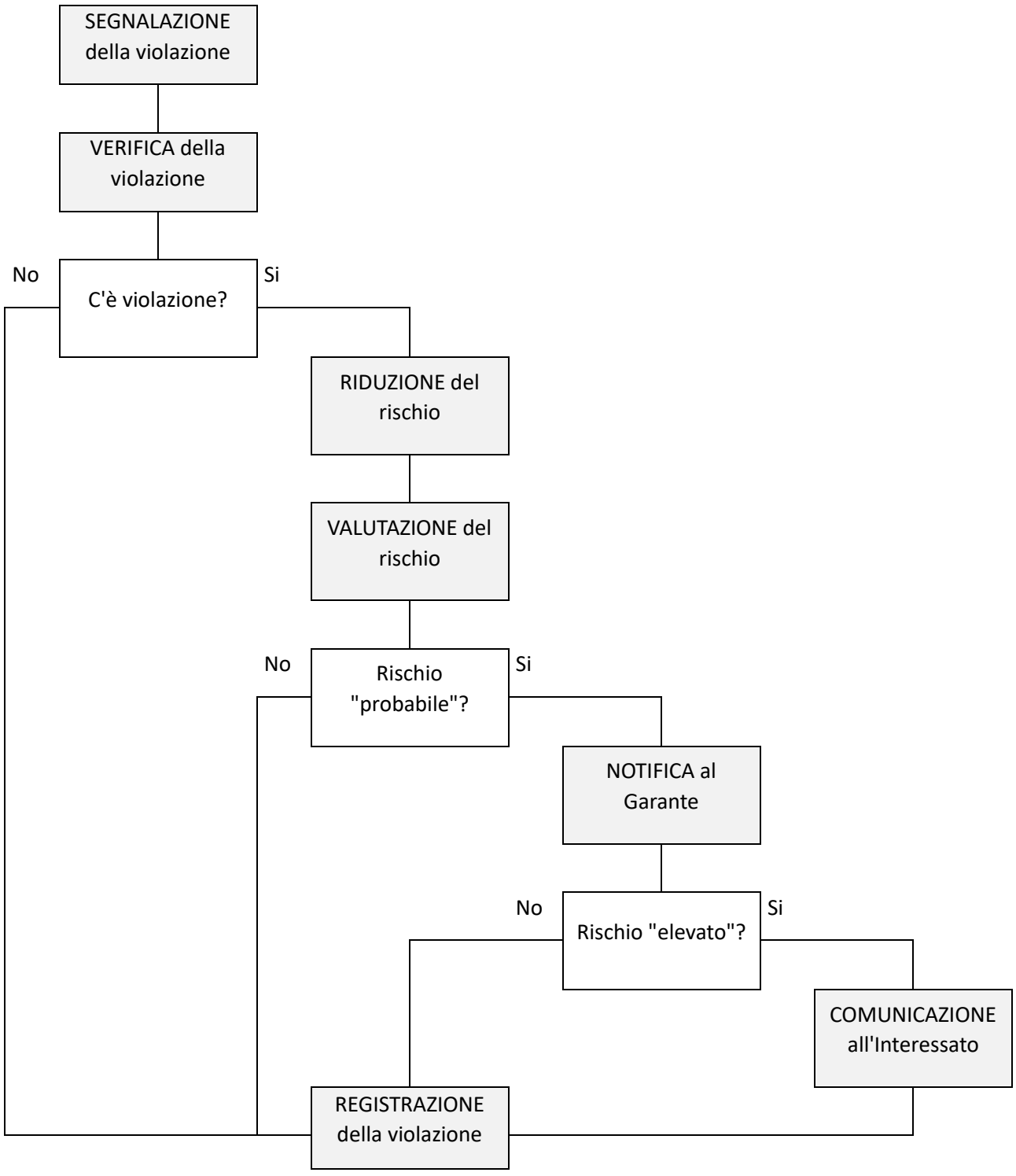
Responsabile esterno: ai sensi dell'art.28 GDPR, ogni fornitore di servizi che tratta dati personali per conto del Titolare sulla base di un contratto o altro atto giuridico equivalente stipulato tra Titolare e Responsabile esterno.

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)

PROVINCIA DI PIACENZA

Ufficio di staff Personale, affari generali, contratti

PARERE DI REGOLARITA' TECNICA

Sulla proposta n. 435/2024 del Ufficio Personale ad oggetto: REGOLAMENTO UE 2016/679 GENERAL DATA PROTECTION REGULATION (GDPR) - APPROVAZIONE DELLA PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI, si esprime ai sensi dell'art. 49, 1° comma del Decreto legislativo n. 267 del 18 agosto 2000, parere FAVOREVOLE in ordine alla regolarità tecnica.

Piacenza lì, 22/03/2024

Sottoscritto dal Dirigente
(TERRIZZI LUIGI)
con firma digitale

PROVINCIA DI PIACENZA

Servizio Personale e Affari Generali

Relazione di Pubblicazione

Determina N. 41 del 25/03/2024

Ufficio di staff Personale, affari generali, contratti

Oggetto: REGOLAMENTO UE 2016/679 GENERAL DATA PROTECTION REGULATION (GDPR) - APPROVAZIONE DELLA PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI.

La su estesa determinazione viene oggi pubblicata all'Albo Pretorio per quindici giorni consecutivi ai sensi dell'art. 52 comma 1 dello Statuto vigente.

Piacenza li, 26/03/2024

Sottoscritta per il Dirigente del Servizio
Il funzionario delegato
(CAPRA MONICA)
con firma digitale