COMUNE DI PRIMIERO
SAN MARTINO DI CASTROZZA

Provincia di Trento

Verbale di deliberazione N. 276

della Giunta comunale

OGGETTO: **Artt. 33 e 34 del Regolamento (UE) 2016/679. Modifica della procedura adottata per la gestione delle violazioni dei dati personali (Data Breach).**

L'anno **DUEMILAVENTICINQUE** addì **nove** del mese di **ottobre**, alle ore 16.00, nella sala delle riunioni, a seguito di regolari avvisi, recapitati a termine di legge, si è convocata la Giunta comunale.

Presenti i signori:

	Assenti	
	giust.	ingiust.
1. Depaoli Daniele - Sindaco		
2. Secco Paolo - Assessore	X	
3. Tisot Martino - Assessore	X	
4. Zagonel Walter - Assessore		
5. Zanetel Mariangela - Assessore		
6. Zortea Giacobbe - Assessore		

Assiste il Segretario Comunale Zurlo dott.ssa Sonia.

Riconosciuto legale il numero degli intervenuti, il Signor Depaoli Daniele, nella sua qualità di Sindaco assume la presidenza e dichiara aperta la seduta per la trattazione dell'oggetto suindicato.

OGGETTO: Artt. 33 e 34 del Regolamento (UE) 2016/679. Modifica della procedura adottata per la gestione delle violazioni dei dati personali (Data Breach).

LA GIUNTA COMUNALE

Premesso che:

- in data 25.05.2018 è entrato in vigore il Regolamento (UE) 2016/679 del Parlamento Europeo, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati, che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- tale Regolamento – denominato "*Regolamento generale sulla protezione dei dati*", in sigla GDPR – detta la nuova disciplina in materia del trattamento dei dati personali, prevedendo tra gli elementi caratterizzanti e innovativi il "*principio di responsabilizzazione*" (c.d. accountability);
- in data 19.09.2018 è entrato in vigore il D.Lgs 10.08.2018 n. 101 di armonizzazione al Regolamento (UE) 2016/679;
- con deliberazione n. 133 di data 07.05.2018 è stato affidato al Consorzio dei Comuni Trentini, quale società "*in house providing"*, il "*Servizio di Responsabile della protezione dei dati personali (RPD*)" nel rispetto della vigente normativa.

Dato atto che, a seguito dell'entrata in vigore del Regolamento (UE) 2016/679 e ss.mm., il Comune di Primiero San Martino di Castrozza è tenuto ad assicurare una serie di adempimenti finalizzati a dare completa esecuzione alla norma;
considerato che tra uno degli adempimenti è quello previsto dagli artt. 33 e 34 del Regolamento (UE) 2016/679, che prevede l'adozione da parte di aziende e Pubbliche Amministrazioni di un piano di protezione dei dati personali che, partendo dall'analisi della mappatura e dall'analisi dei trattamenti, effettui la valutazione del rischio di violazione ed individui le misure volte ad eliminare o almeno ridurre il rischio stesso e in fine preveda un procedura per la gestione delle violazioni dei dati personali ("Data Breach");
visto lo schema di procedura per la gestione delle violazioni dei dati personali ("Data Breach") predisposto dal Consorzio dei Comuni Trentini e approvato con Deliberazione della Giunta comunale n. 404 di data 16.12.2019, comprensiva della seguente documentazione:

- flusso degli adempimenti in caso di violazione dei dati;
- modello di potenziale violazione dei dati personali al Responsabile Protezione Dati;
- modello comunicazione violazione all'Autorità Garante;

preso atto che in data 27.05.2021 il Garante per la Protezione dei Dati Personali ha approvato una nuova Procedura telematica per la notifica di violazioni di dati personali (data breach), con provvedimento n. 209-2021, modificando il contenuto e le modalità della notifica delle violazioni dei dati personali individuati nel provvedimento n. 157 dd. 30.06.2019 ed adottando un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità all'indirizzo "https://servizi.gpdp.it/", attraverso la quale i titolari del trattamento forniscono al Garante le informazioni ivi richieste, ai sensi dell'art. 33 del Regolamento e dell'art. 26 del Decreto;
considerato che si rende quindi necessario approvare una modifica alla procedura adottata per la gestione delle violazioni dei dati personali (Data Breach) attualmente in vigore, modificando i punti n. 5 "*Gestione delle attività conseguenti ad una possibile violazione di dati personali*" e n. 6 "*Notifica della violazione dei dati personali all'Autorità Garante*";
più precisamente al punto n. 5

[...]

- *condurre e documentare un'indagine corretta e imparziale sull'evento (aspetti organizzativi, informatici, legali, ecc.) attraverso la compilazione del "Modello di potenziale violazione di dati personali al*

Responsabile Protezione Dati" viene modificato in *"[...] condurre e documentare un'indagine corretta e imparziale sull'evento (aspetti organizzativi, informatici, legali, ecc.) e successivamente documentare e notificare la violazione al Garante Privacy per la protezione dei dati personali tramite apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità e raggiungibile al seguente indirizzo https://servizi.gpdp.it/databreach/s/";*

- *"riferire i risultati dell'indagine inviando il modello all'indirizzo serviziorpd@comunitrentini.it al Responsabile della Protezione dei Dati, al Referente privacy dell'Ente e il Titolare*", viene modificato in "*riferire i risultati dell'indagine all'indirizzo serviziorpd@comunitrentini.it al Responsabile della Protezione dei Dati, al Referente privacy dell'Ente e il Titolare*".

Al punto n. 6 *"Il Titolare, tenuto conto del parere formulato dal Responsabile della Protezione dei Dati, e dalle valutazioni fatte congiuntamente dal Referente della gestione delle violazioni dei dati personali e dal Referente Privacy dell'Ente, se ritiene accertata la violazione dei dati personali e che la stessa possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche, notifica tale violazione avvalendosi del "Modello comunicazione violazione all'Autorità Garante"* diventa *"Il Titolare, tenuto conto del parere formulato dal Responsabile della Protezione dei Dati, e dalle valutazioni fatte congiuntamente dal Referente della gestione delle violazioni dei dati personali e dal Referente Privacy dell'Ente, se ritiene accertata la violazione dei dati personali e che la stessa possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche, notifica tale violazione al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/"*;
esaminata la proposta di cui trattasi e ritenuta la stessa meritevole di approvazione in quanto rispondente alle finalità ed ai contenuti degli artt. 33 e 34 del Regolamento (UE) 2016/679.

Visti:
- il Codice degli Enti Locali della Regione autonoma Trentino Alto-Adige approvato con Legge regionale 03.05.2018, n. 2;
- il D.Lgs. 10.08.2018 n. 101;
- il Regolamento (UE) 2016/679, e in particolare gli artt. 33 e 34;
- lo Statuto comunale;
- il Regolamento per la disciplina dei controlli interni, approvato con deliberazione consiliare n. 4 del 02.02.2017 e di questi in particolare il Capo II – Controlli di regolarità amministrativa e contabile;
- la deliberazione del Consiglio comunale n. 68 del 18.12.2024 con la quale è stato approvato il Documento Unico di Programmazione (DUP) 2025-2027 e il bilancio di previsione 2025-2027 e ss. mm.;
- il P.E.G. per la gestione del Bilancio per l'anno 2025 approvato con deliberazione della Giunta Comunale n. 381 del 30.12.2024;
- il PIAO approvato con deliberazione della Giunta Comunale n. 25 del 04.02.2025;

verificato che l'adozione della presente deliberazione rientra nella competenza della Giunta comunale ai sensi dell'art. 53 della Legge regionale 3 maggio 2018 n. 2 e s.m.;
acquisito il parere favorevole espresso dal Segretario comunale in ordine alla regolarità tecnico-amministrativa del presente atto espresso ai sensi dell'art. 185 del Codice degli Enti Locali della Regione autonoma Trentino Alto-Adige approvato con Legge regionale 3 maggio 2018, n. 2;
dato atto che la presente deliberazione non comporta l'assunzione di alcun impegno di spesa e che pertanto, non si rende necessario acquisire il parere di regolarità contabile né il visto di copertura finanziaria;
con voti favorevoli unanimi espressi nelle forme di legge;

DELIBERA

1. Di approvare, per le motivazioni esposte in premessa, la modifica dei punti n. 5 "*Gestione delle attività conseguenti ad una possibile violazione di dati personali*" e n. 6 "*Notifica della violazione dei dati personali all'Autorità Garante*" della procedura disciplinante la gestione delle violazioni dei dati personali ("Data Breach") di cui agli artt. 33 e 34 del Regolamento (UE) 2016/679, che si allega alla presente deliberazione, di cui forma parte integrante e sostanziale.
   Più precisamente al punto n. 5 *"*

   [...]

   - *condurre e documentare un'indagine corretta e imparziale sull'evento (aspetti organizzativi, informatici, legali, ecc.) attraverso la compilazione del "Modello di potenziale violazione di dati personali al Responsabile Protezione Dati"* viene modificato in *"[...] condurre e documentare un'indagine corretta e imparziale sull'evento (aspetti organizzativi, informatici, legali, ecc.) e successivamente documentare e notificare la violazione al Garante Privacy per la protezione dei dati personali tramite apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità e raggiungibile al seguente indirizzo https://servizi.gpdp.it/databreach/s/";*
   - *"riferire i risultati dell'indagine inviando il modello all'indirizzo serviziorpd@comunitrentini.it al Responsabile della Protezione dei Dati, al Referente privacy dell'Ente e il Titolare*", viene modificato in "*riferire i risultati dell'indagine all'indirizzo serviziorpd@comunitrentini.it al Responsabile della Protezione dei Dati, al Referente privacy dell'Ente e il Titolare*".

   Al punto n. 6 *"Il Titolare, tenuto conto del parere formulato dal Responsabile della Protezione dei Dati, e dalle valutazioni fatte congiuntamente dal Referente della gestione delle violazioni dei dati personali e dal Referente Privacy dell'Ente, se ritiene accertata la violazione dei dati personali e che la stessa possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche, notifica tale violazione avvalendosi del "Modello comunicazione violazione all'Autorità Garante"* diventa *"Il Titolare, tenuto conto del parere formulato dal Responsabile della Protezione dei Dati, e dalle valutazioni fatte congiuntamente dal Referente della gestione delle violazioni dei dati personali e dal Referente Privacy dell'Ente, se ritiene accertata la violazione dei dati personali e che la stessa possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche, notifica tale violazione al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/".*
2. Di dare atto che la procedura di cui al precedente punto 1) risulta comprensiva della seguente documentazione che sarà aggiornata in base alle modifiche della normativa in materia:
   - flusso degli adempimenti in caso di violazione dei dati.
3. Di incaricare il Segretario comunale, nella sua qualità di Referente privacy del Comune di Primiero San Martino di Castrozza di garantire un'adeguata informazione al personale dipendente in ordine alla procedura di cui al primo punto.
4. Di comunicare la presente deliberazione al Consorzio dei Comuni Trentini, nella persona del Responsabile della protezione dei dati del Comune di Primiero San Martino di Castrozza.
5. Di dichiarare questo atto esecutivo a pubblicazione avvenuta.
6. Di dare evidenza, ai sensi dell'art. 4 della L.P. 30 novembre 1992, n. 23 e ss. mm., che avverso la presente deliberazione sono ammessi:
   - opposizione alla Giunta comunale, durante il periodo di pubblicazione, ai sensi dell'art. 183, quinto comma, del Codice degli Enti Locali della Regione autonoma Trentino Alto-Adige approvato con Legge regionale 3 maggio 2018, n. 2;
   - ricorso giurisdizionale al Tribunale Regionale di Giustizia amministrativa entro 60 giorni ai sensi dell'art. 29 dell'allegato 1) del D.Lgs. 02/07/2010 n. 104;
   - ricorso straordinario al Presidente della Repubblica, entro 120 giorni, ai sensi dell'art. 8 del D.P.R. 24 novembre 1971, n° 1199.

Data lettura del presente verbale, lo stesso viene approvato e sottoscritto.

IL SINDACO	IL SEGRETARIO COMUNALE
Depaoli Daniele	Zurlo dott.ssa Sonia

Documento prodotto in originale informatico e firmato digitalmente ai sensi degli art. 20 e 21 del "Codice dell'amministrazione digitale" (D.Leg.vo 82/2005).

COMUNE DI PRIMIERO
SAN MARTINO DI CASTROZZA
Provincia di Trento

SERVIZIO RESPONSABILE DELLA PROTEZIONE DEI DATI

PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Documento approvato con Deliberazione della Giunta comunale n. 404 di data 16.12.2019
Documento modificato con Deliberazione della Giunta comunale n. 000 di data 00.10.2025

38054 Fiera di Primiero – via Fiume,10
Tel 0439 762161 – e-mail protocollo@comuneprimiero.tn.it
e –mail cert. comune@pec.comuneprimiero.tn.it
Cod. fisc. Part. Iva 02401890229

INDICE

1 Scopo

Il presente documento contiene le indicazioni, le responsabilità e le azioni da attuare per la gestione della procedura da attivare in caso di possibile violazione dei dati personali, in osservanza agli obblighi relativi alla notifica all'Autorità Garante per la protezione dei dati personali e alla comunicazione all'interessato, in ossequio alle previsioni di cui agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016.

Tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali dell'Ente devono essere informati e osservare la presente Procedura.

2 Aggiornamento

Il Referente privacy dell'Ente, nel caso di variazioni organizzative e/o normative, aggiorna la presente procedura e la propone in approvazione all'Organo competente affinché la renda esecutiva.

3 Definizioni

Le seguenti definizioni dei termini utilizzati in questo documento sono tratte dall'articolo 4 del Regolamento europeo n. 679 del 2016:

«**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;

«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

«violazione dei dati personali»: 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 in formato elettronico e/o cartaceo;

«**Responsabile della Protezione dei Dati**»: incaricato di assicurare la corretta gestione dei dati personali nell'Ente;

«Autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR dell'UE.

4 Organizzazione delle attività di gestione dell'evento violazione dei dati personali

Il Titolare deve:

- designare un Referente della gestione delle violazioni dei dati personali (di seguito Referente data breach), figura che potrebbe coincidere con il Referente privacy dell'Ente;
- comunicare i nomi dei designati a tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali dell'Ente;
- avvalendosi del Referente data breach, predisporre il Registro delle violazioni dei dati personali.

5 Gestione delle attività conseguenti ad una possibile violazione di dati personali

Il soggetto che, a diverso titolo o in quanto autorizzato al trattamento di dati personali di cui è titolare l'Ente, viene a conoscenza di una possibile violazione dei dati personali, deve immediatamente segnalare l'evento al Referente Privacy dell'Ente e al Referente data breach e fornire loro la massima collaborazione.

La mancata segnalazione del suddetto evento comporta a diverso titolo responsabilità a carico del soggetto che ne è a conoscenza.

Il Referente data breach, se del caso avvalendosi del Gruppo di gestione delle violazioni dei dati personali, deve:

- adottare le Misure di sicurezza informatiche e/o organizzative per porre rimedio o attenuare i possibili effetti negativi della violazione dei dati personali e, contestualmente, informare immediatamente il Responsabile della Protezione dei Dati per una valutazione condivisa;
- condurre e documentare un'indagine corretta e imparziale sull'evento (aspetti organizzativi, informatici, legali, ecc.) e successivamente documentare e notificare la violazione al Garante Privacy per la protezione dei dati personali tramite apposita procedura telematica, resa

disponibile nel portale dei servizi online dell'Autorità e raggiungibile al seguente indirizzo https://servizi.gpdp.it/databreach/s/.

- riferire i risultati dell'indagine all'indirizzo serviziorpd@comunitrentini.it al Responsabile della Protezione dei Dati, al Referente privacy dell'Ente e il Titolare.

Il Responsabile della Protezione dei Dati, ricevuti i risultati dell'indagine, analizza l'accaduto e formula un parere in merito all'evento, esprimendo la propria valutazione, non vincolante, che lo stesso configuri in una violazione dei dati personali e che possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche.

Lo invia quindi al Referente data breach che lo mette a conoscenza del Referente privacy dell'Ente e il Titolare.

6 Notifica della violazione dei dati personali all'Autorità Garante

Il Titolare, tenuto conto del parere formulato dal Responsabile della Protezione dei Dati, e dalle valutazioni fatte congiuntamente dal Referente della gestione delle violazioni dei dati personali e dal Referente Privacy dell'Ente, se ritiene accertata la violazione dei dati personali e che la stessa possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche, notifica tale violazione al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/.

La notifica deve essere effettuata senza ingiustificato ritardo dall'accertamento dell'evento e, ove possibile, entro 72 ore dall'accertamento dello stesso con le modalità e i contenuti previsti dall'art. 33 del Regolamento europeo n. 679 del 2016.

7 Comunicazione della violazione dei dati personali agli interessati

Il Titolare, accertata la violazione dei dati personali e ritenendo che la stessa possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte, oltre alla notifica di cui al punto 6, decide le modalità di comunicazione di tale violazione agli interessati, come previsto dall'art. 34 del Regolamento europeo n. 679 del 2016.

8 Compilazione del Registro delle violazioni dei dati personali

Il Titolare, avvalendosi del Referente data breach, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nel Registro delle violazioni dei dati personali.

Tale documento è tenuto e implementato dal Referente data breach e consente all'autorità di controllo di verificare il rispetto dall'art. 33 del Regolamento europeo n. 679 del 2016.

Per la redazione del registro è possibile ricorrere al sistema di fascicolazione se disponibile nel programma di gestione documentale dell'Ente o ad un file excel.

Il flusso degli adempimenti in caso di violazione dei dati