COMUNE DI MEZZANA

(Provincia di Trento)

Verbale di deliberazione N. 52

della Giunta comunale

OGGETTO: **Articoli 33 e 34 del Regolamento UE 2016/679. Adozione della procedura per la gestione delle violazioni dei dati personali (DATA BREACH) e istituzione Registro data breach.**

L'anno **DUEMILAVENTISEI** addì **diciannove** del mese di **maggio**, alle ore 10.00, nella sala delle riunioni, presso la sede Municipale di Mezzana, a seguito di regolari avvisi, recapitati a termine di legge, si è convocata la Giunta comunale.

.

Presenti i signori:

	Assenti	
	giust.	ingiust.
1. Redolfi Giacomo - Sindaco		
2. Pasquali Mario - Vicesindaco		
3. Dalla Valle Irene - Assessore		
4. Gosetti Luca - Assessore		
5. Barbetti Roberta - Assessore		

Assiste il Segretario Comunale Signora Michelotti dott.ssa Monica.

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

Oggetto: Articoli 33 e 34 del Regolamento UE 2016/679. Adozione della procedura per la gestione delle violazioni dei dati personali (DATA BREACH) e istituzione Registro data breach.

LA GIUNTA COMUNALE

Premesso che in data 25.05.2018 è entrato in vigore il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio di data 27.04.2016, 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) e rilevato inoltre che in data 19.09.2018 è entrato in vigore il D.Lgs. 10.08.2018 n. 101 di armonizzazione al Regolamento (UE) 2016/679.

Evidenziato che il Regolamento (UE) 2016/679 - denominato "*Regolamento generale sulla protezione dei dat*i", in sigla RGPD - detta una nuova disciplina in materia di trattamento dei dati personali, prevedendo tra gli elementi caratterizzanti e innovativi il "principio di responsabilizzazione" (c.d. *accountability*) e ponendo al centro del nuovo quadro normativo la figura del "Responsabile della protezione dei dati", in sigla RPD**.**

Ricordato che il Comune di Mezzana:

- con deliberazione della Giunta comunale n. 10 di data 23 gennaio 2024 ha affidato al Consorzio dei Comuni Trentini il servizio di Responsabile della Protezione dei Dati (RPD) – anno 2024;
- con decreto sindacale n. 2 di data 24 gennaio 2024 stato designato il Consorzio dei Comuni Trentini come Responsabile della Protezione dei Dati (RPD) e individuato il Referente nella dott.ssa Laura Marinelli. Il nominativo e i dati di contatto del RPD sono stati comunicati al Garante per la protezione dei dati personali e pubblicati sul sito istituzionale;
- con deliberazione della Giunta comunale n. 98 di data 20 novembre 2025, il Comune di Mezzana, in continuità con gli anni precedenti, ha affidato il servizio di consulenza in materia di privacy attivato dal Consorzio dei Comuni Trentini a seguito dell'entrata in vigore del nuovo regolamento europeo 2016/679 con particolare riferimento alla figura del Responsabile della Protezione dei dati (RPD).

Verificato che il Comune di Mezzana è tenuto, a seguito dell'entrata in vigore del Regolamento (UE) 2016/679, ad una serie di adempimenti conseguenti.

Accertato come tra gli adempimenti sopra indicati rientri quello previsto dagli articoli 33 e 34 del Regolamento (UE) 2016/679, e segnatamente:

- quello relativo all'adozione di una specifica procedura disciplinante la gestione delle violazioni dei dati personali (*data breach*);
- quello relativo all'istituzione di un registro interno data breach, dove vengono annotate sia le violazioni non notificabili che quelle notificabili, il quale deve contenere 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, è necessario istituire:

- una Procedura data breach
- un registro interno data breach, dove vengono annotate sia le violazioni non notificabili che quelle notificabili.

Dato atto che, nell'ambito Servizio di consulenza in materia di "privacy" il Consorzio dei Comuni Trentini s.c.a.r.l. ha elaborato una proposta di procedura disciplinante la gestione delle violazioni dei dati personali ("data breach"), composta dei seguenti allegati:

- procedura per la gestione della violazione dei dati personali;
- modello di potenziale violazione dei dati personali al Responsabile Protezione Dati;
- registro delle violazioni.

Esaminata la proposta di cui trattasi e ritenuta la stessa meritevole di approvazione in quanto rispondente alle finalità ed ai contenuti previsti dagli articoli 33 e 34 del Regolamento (UE) 2016/679**.**

Stabilito di demandare al Sindaco, nella sua qualità di Titolare del trattamento, la effettuazione della designazione del Referente della gestione delle violazioni dei dati personali ("Referente data breach").

Dato atto che con deliberazione del Consiglio Comunale n. 40 di data 29 dicembre 2025, sono stati approvati il Documento Unico di Programmazione (DUP) 2026-2028, il bilancio di previsione finanziario 2026-2027-2028, la nota integrativa e il piano degli indicatori e dei risultati attesi di bilancio.

Visti i successivi provvedimenti di variazione.

Visto il Decreto Sindacale n. 13 di data 31 dicembre 2025 relativo alla nomina dei Responsabili dei Servizi per l'anno 2026, così come modificato dal decreto sindacale n. 4 di data 4 maggio 2026.

Preso atto che con deliberazione della Giunta Comunale n. 4 di data 13 gennaio 2026, dichiarata immediatamente eseguibile, è stato approvato il Piano Esecutivo di Gestione (P.E.G.) 2026-2028 – parte finanziaria (ex art. 169 D.Lgs. 18 agosto 2000 n. 267 e ss.mm.).

Precisato che con deliberazione della Giunta Comunale n. 38 di data 26 marzo 2026, dichiarata immediatamente eseguibile, è stato approvato il Piano Integrato di Attività e Organizzazione 2026/2028.

Acquisito sulla proposta di deliberazione il parere in ordine alla regolarità tecnico-amministrativa reso dal Segretario Comunale, espresso ai sensi dell'articolo 185 del Codice degli Enti Locali della Regione Autonoma Trentino-Alto Adige approvato con Legge Regionale di data 03 maggio 2018, n. 2.

Considerato che il presente atto non ha rilevanza in termini contabili e pertanto non necessita del parere di regolarità contabile del Responsabile del Servizio Finanziario**.**

Visto lo Statuto comunale, approvato con deliberazione consiliare n° 9 dd. 20.02.2007 e s.m. e i.

Vista la Legge Regionale di data 29 ottobre 2014, n. 10 e s.m. e i., con la quale si adeguavano gli obblighi di pubblicità, trasparenza e diffusione di informazioni da osservare da parte della Regione T.A.A. e degli Enti a ordinamento regionale, come già individuati dalla Legge di data 06 novembre 2012, n. 190 e dal Decreto Legislativo di data 14 marzo 2013, n. 33.

Visto il Codice degli Enti Locali della regione Autonoma Trentino-Alto Adige approvato con legge Regionale 3 maggio 2018 n. 2 e ss.mm..

Con voti favorevoli unanimi espressi nelle forme di legge,

D E L I B E R A

1. Di adottare, per le motivazioni esposte in premessa, la procedura disciplinante la gestione delle violazioni dei dati personali ("data breach") di cui agli arti. 33 e 34 del Regolamento (UE) 2016/679, allegata alla presente deliberazione formandone parte integrante e sostanziale.
2. Di dare atto che la procedura di cui al precedente punto 1) risulta comprensiva dei seguenti allegati:
   - procedura per la gestione della violazione dei dati personali;
   - modello di potenziale violazione dei dati personali al Responsabile Protezione Dati;
   - registro delle violazioni.
3. Di demandare al Sindaco, nella sua qualità di Titolare del trattamento, la effettuazione della designazione del Referente della gestione delle violazioni dei dati personali ("Referente data breach").
4. Di incaricare il Segretario Comunale, nella sua qualità di Referente privacy dell'ente, di garantire una adeguata informazione al personale dipendente in ordine alla Procedura per la gestione del data breach.
5. Di comunicare la presente deliberazione al Consorzio dei Comuni Trentini, in qualità di RPD.
6. Di disporre la comunicazione del presente provvedimento, contestualmente all'affissione all'Albo Comunale, ai capigruppo consiliari, ai sensi dell'articolo 183 comma 2 del Codice degli Enti Locali della Regione Autonoma Trentino-Alto Adige approvato con Legge Regionale di data 03 maggio 2018, n. 2.
7. Di dare evidenza che ai sensi dell'art. 4 della L.P. 30.11.1992 n. 23 avverso il presente atto sono ammessi:
   - opposizione, da parte di ogni cittadino, alla Giunta Comunale durante il periodo di pubblicazione ai sensi dell'art. 183, comma 5 del C.E.L. approvato con L.R. 3 maggio 2018 n. 2;

- Ricorso giurisdizionale al Tribunale Regionale di Giustizia Amministrativa di Trento entro 60 giorni, ai sensi degli artt. 13 e 29 del D.Lgs. 02.07.2010 n. 104.
  ovvero ed in alternativa al ricorso giurisdizionale
- Ricorso straordinario al Presidente della Repubblica, ai sensi dell'art. 8 del D.P.R. 24.11.1971 n. 1199, entro 120 giorni dalla data della notifica o della comunicazione, o da quando l'interessato ne abbia avuto piena conoscenza.

8. Di dare atto che la presente deliberazione diverrà esecutiva a pubblicazione avvenuta ai sensi dell'articolo 183 comma 3 del Codice degli Enti Locali della Regione Autonoma Trentino-Alto Adige approvato con Legge Regionale di data 03 maggio 2018, n. 2 e che ad essa va data ulteriore pubblicità, quale condizione integrativa d'efficacia, sul sito internet del Comune per un periodo di 5 anni, ai sensi della L.R. 29 ottobre 2014, n. 10 e s.m. e i., nei casi previsti dal Decreto Legislativo n. 33 del 14 marzo 2013 e dalla Legge 06 novembre 2012, n. 190.

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

IL SINDACO	IL SEGRETARIO COMUNALE
Redolfi Giacomo	Michelotti dott.ssa Monica

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).

Provincia di Trento

COMUNE DI MEZZANA

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

Documento approvato con Delibera n. 52 di data 19.05.2026

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 nominativi del Referente privacy e del Referente data breach a tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali dell'Ente;
- nel caso di modifica/sostituzione dei soggetti preposti il titolare provvede a comunicare i nuovi nominativi 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 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.) attraverso la compilazione del "Modello di potenziale violazione di dati personali al Responsabile Protezione Dati";
- condividere con il Referente privacy e il Titolare i risultati dell'indagine;
- riferire i risultati dell'indagine al Responsabile della Protezione dei Dati inviando il "modello di potenziale violazione di dati personali al Responsabile Protezione Dati" compilato all'indirizzo serviziorpd@comunitrentini.it.

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.

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 avvalendosi della procedura telematica disponibile al seguente link: https://www.garanteprivacy.it/data-breach.
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.

POTENZIALE VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL RESPONSABILE DELLA PROTEZIONE DEI DATI

Ente _____

Referente Privacy _____

Telefono _____ **Email** _____

Breve descrizione della violazione dei dati personali

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

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

- ☐ Il _____
- ☐ Tra il _____ e il _____
- ☐ In un tempo non ancora determinato
- ☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei 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 non li ha l'autore della violazione)
- ☐ Altro _____

Dispositivo o strumento oggetto della violazione

- ☐ Computer
- ☐ Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di backup
- ☐ Documento cartaceo
- ☐ Software _____
- ☐ Servizio informatico _____
- ☐ Altro _____

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ Numero _____ di persone
- ☐ Circa _____ persone
- ☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

- ☐ Dati anagrafici/codice fiscale
- ☐ Dati di accesso e di identificazione (*username, password, customer ID, altro*)
- ☐ Dati relativi a minori

- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico, o sindacale
- ☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- ☐ Dati giudiziari
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ Altro _____

Fornitori o soggetti esterni coinvolti

Misure tecniche, informatiche e organizzative applicate ai dati oggetto di violazione

Luogo e data _____

Firma _____

Registro delle violazioni dei dati DEL Comune di Mezzana

NR.	Data accadimento	Data comunicazione al referente interno	Breve descrizione evento	Servizio/Ufficio competente al trattamento	Coinvolgimento RPD: SI/NO	Azioni / Misure adottate	Notifica al Garante SI/NO e data	Comunicazione agli interessati SI/NO e data
1								
2								
3								
4								
5								
6								