COPIA

# COMUNE DI TESERO

Registro deliberazioni n. 41 / 2026

## VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

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

Il giorno cinque marzo 2026, alle ore 14.45 nella sala delle sedute del Municipio, in seguito di regolari avvisi, recapitati a termine di legge, si è convocata la Giunta comunale.

Presenti i signori:

Deflorian Massimiliano - SINDACO
Barbolini Alan - VICESINDACO
De Zolt Simona - ASSESSORE
Zanon Elena - ASSESSORE
Volcan Enrico - ASSESSORE

Assenti i signori:

Assiste e verbalizza il Segretario Comunale Signora **Luchini dott.ssa Chiara**.

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

Oggetto: Art. 33 e 34 del Regolamento (UE) 2016/679. Aggiornamento della procedura 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 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 dei dati, e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- 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 come il Regolamento (UE) 2016/679 - denominato "*Regolamento generale sulla protezione dei dati*" detti 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.

Rilevato, a tal proposito, che:

- con deliberazione della Giunta comunale n. 66 dd. 19.04.2018, è stato affidato al Consorzio dei Comuni Trentini il "Servizio Responsabile della protezione dei dati personali (RPD)" nel rispetto della vigente normativa, in quanto società in house providing, rinnovato successivamente nel corso degli anni, da ultimo con deliberazione della Giunta comunale n. 227 dd. 04.12.2025 per il 2026;
- che a seguito di modifica in data 08.01.2024 prot. 146, è stato designato il Consorzio dei Comuni Trentini quale Responsabile della protezione dei dati personali del medesimo Comune di cui all'art. 37 del Regolamento (UE) 2016/679.

Sottolineato come il Comune di Tesero sia 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 artt. 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").

Richiamata la precedente deliberazione giuntale n. 240 di data 13.12.2018 con la quale si procedeva a adottare la procedura per la gestione delle violazioni dei dati personali cosiddetta "Data Breach", comprensiva dei modelli di comunicazione della violazione all'Autorità Garante e al Responsabile della Protezione dei Dati.

Considerato che il Provvedimento del Garante n. 209 del 27 maggio 2021 e le Linee Guida EDPB n. 1/2021 e n. 9/2022 hanno introdotto una nuova modalità di notifica delle violazioni di dati personali all'Autorità Garante, rendendo obbligatorio, dal 1° luglio 2021, l'utilizzo della procedura telematica, rendendo necessario l'adeguamento della procedura esistente.

Precisato, inoltre, che nell'ultimo incontro annuale effettuato con il Servizio RPD del Consorzio dei Comuni Trentini, è emersa pertanto la necessità di effettuare suddetta modifica alla procedura per la gestione delle violazioni dei dati personali ("data breach") e ritenuto doveroso riapprovarla.

Preso atto che previa consulenza del Servizio RPD del Consorzio dei Comuni Trentini gli uffici comunali hanno predisposto, a tal fine, una proposta di modifica della procedura disciplinante la gestione delle violazioni dei dati personali ("data breach").

Evidenziato che la suddetta procedura prevede anche il modello di potenziale violazione dei dati personali da inviare al Responsabile Protezione Dati.

Esaminata la suddetta proposta e ritenuta meritevole di condivisione e approvazione in quanto rispondente alle finalità ed ai contenuti previsti dagli artt. 33 e 34 del Regolamento (UE) 2016/679.

Evidenziato che il Referente della gestione delle violazioni dei dati personali ("Referente data breach") è il Segretario comunale.

Visto il Regolamento (UE) 2016/679, e in particolare gli artt. 33 e 34.

Visto il D.Lgs. 10.08.2018 n. 101.

Visto lo Statuto comunale approvato con deliberazione del Consiglio comunale n. 441 di data 26.01.1994 e da ultimo modificato ed aggiornato con deliberazione del Consiglio comunale n. 4 di data 20.04.2016.

Visto il Codice degli Enti Locali della Regione Autonoma Trentino-Alto Adige approvato con L.R. 3 maggio 2018 n. 2.

Acquisiti preventivamente, sulla proposta di deliberazione, i pareri favorevoli previsti dalle disposizioni dell'art. 185 del Codice degli Enti Locali della Regione Autonoma Trentino-Alto Adige approvato con L.R. 3 maggio 2018 n. 2, che vengono allegati al presente provvedimento (parere di regolarità tecnica).

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 modifica alla procedura disciplinante la gestione delle violazioni dei dati personali ("data breach") di cui agli artt. 33 e 34 del Regolamento (UE) 2016/679, secondo le indicazioni fornite dal Consorzio dei Comuni Trentini Servizio RPD.

2. Di dare atto che tale procedura è composta anche dal modello di potenziale violazione dei dati personali al Responsabile Protezione Dati, quale parte integrante e sostanziale alla presente deliberazione.

3. Di predisporre, altresì, un registro delle violazioni nel quale andranno annotate le violazioni dei dati occorse.

4. Di inviare il suddetto provvedimento al Servizio RPD del Consorzio dei Comuni Trentini.

5. Di inviare il suddetto provvedimento, altresì, per opportuna conoscenza a tutto il personale dipendente e agli amministratori comunali.

*Ai sensi dell'art. 4, comma 4, della L.P. 30.11.1992, n. 23, avverso il presente provvedimento è possibile presentare:*

- *opposizione, da parte di ogni cittadino, alla Giunta comunale, entro il periodo di pubblicazione, ai sensi dell'art. 183, comma 5, del Codice degli Enti Locali della Regione Autonoma Trentino-Alto Adige, approvato con L.R. 03.05.2018, n. 2;*
- *ricorso giurisdizionale al T.R.G.A., entro 60 giorni, ai sensi dell'art. 29 del D.Lgs. 02.07.2010, n. 104;*
- *in alternativa alla possibilità indicata sopra, ricorso straordinario al Presidente della Repubblica, entro 120 giorni, ai sensi dell'art. 8 del D.P.R. 24.11.1971, n. 1199.*

*Gli atti delle procedure di affidamento relativi a pubblici lavori, servizi o forniture, ivi comprese le procedure di affidamento di incarichi di progettazione e di attività tecnico - amministrative ad esse connesse, sono impugnabili unicamente mediante ricorso al T.A.R. di Trento entro 30 giorni, ai sensi degli articoli 119 e 120 del D.Lgs. 02.07.2010, n. 104.*

Data lettura del presente verbale viene approvato e sottoscritto.

Il Sindaco
F.to Massimiliano Deflorian

Il Segretario Comunale
F.to dott.ssa Chiara Luchini

---

**ATTESTATO DI PUBBLICAZIONE**

(Art. 183 comma 3, L.R. 03/05/2018 n. 2)

Si attesta che copia della deliberazione è in pubblicazione per estratto all'albo telematico, giusta attestazione del Funzionario addetto, per 10 giorni consecutivi a partire dal 06/03/2026.

Tesero, 06/03/2026

Il Segretario Comunale
F.to dott.ssa Chiara Luchini

---

**ESECUTIVITA'**

Si certifica che la presente deliberazione è dichiarata esecutiva ad avvenuta pubblicazione, ai sensi dell'art. 183 del Codice degli Enti Locali approvato con L.R. 3 maggio 2018, n. 2.

Il Segretario Comunale
dott.ssa Chiara Luchini

---

**INVIO AI CAPIGRUPPO CONSILIARI**

Ai sensi dell'art. 183, secondo comma, del Codice degli Enti Locali della Regione Trentino Alto - Adige, approvato con L.R. 3 maggio 2018, n. 2, la presente deliberazione viene trasmessa ai capigruppo consiliari.

Tesero, 06/03/2026

Il Segretario Comunale
F.to dott.ssa Chiara Luchini

---

Copia conforme all'originale.

Tesero, 06/03/2026

Il Segretario Comunale
dott.ssa Chiara Luchini

**********

**PARERI OBBLIGATORI ESPRESSI AI SENSI DEGLI ARTICOLI 185 E 187 DEL CODICE DEGLI ENTI LOCALI DELLA REGIONE AUTONOMA TRENTINO ALTO ADIGE APPROVATO CON LEGGE REGIONALE DD. 3 MAGGIO 2018, N. 2**

**PARERE DI REGOLARITÀ TECNICA**

Istruita ed esaminata la proposta di deliberazione in oggetto, come richiesto dagli articoli 185 e 187 del Codice degli enti locali della Regione autonoma Trentino Alto Adige approvato con Legge regionale dd. 3 maggio 2018, n. 2, si esprime parere favorevole in ordine alla regolarità tecnico-amministrativa dell'atto.

Tesero, 05/03/2026

IL SEGRETARIO COMUNALE

F.to Luchini dott.ssa Chiara

**COMUNE DI TESERO**
**PROVINCIA DI TRENTO**
Via 4 Novembre, 27
38038 Tesero (TN)
0462 811700
info@comune.tesero.tn.it
comune@pec.comune.tesero.tn.it

# PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

# (DATA BREACH)

| Documento approvato con Delibera di data | | |
|---|---|---|
| Revisione | Data | Motivo |
| | | |

**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 possibili violazioni 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.

**COMUNE DI TESERO**
**PROVINCIA DI TRENTO**
Via 4 Novembre, 27
38038 Tesero (TN)
0462 811700
info@comune.tesero.tn.it
comune@pec.comune.tesero.tn.it

# 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 _____