COMUNE DI IMER

PROVINCIA DI TRENTO

Verbale di deliberazione N. 124

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 **ventidue** del mese di **ottobre**, alle ore 17.30, nella sede municipale, a seguito di regolari avvisi, recapitati a termine di legge, si è convocata la Giunta comunale.

.

Presenti i signori:

	Assenti	
	giust.	ingiust.
1. Gubert Daniele - Sindaco		
2. Bellotto Gianni - Assessore		
3. Moretta Lorena - Assessore		
4. Romagna Giuseppina - Assessore		
5. Simon Andrea - Assessore		

Assiste il Segretario Comunale Signora Depaoli dott.ssa Francesca.

Riconosciuto legale il numero degli intervenuti, il Signor Gubert 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:

- con precedente deliberazione n. 164 di data 20.12.2018 la Giunta comunale ha approvato la procedura per la gestione delle violazioni dei dati personali "Data Breach", ai sensi del Regolamento (UE) 2016/2018;
- con atto di nomina prot. n. 1939 di data 29.04.2024 è stato individuato il Referente della gestione delle violazioni dei dati personali nella figura del Segretario comunale, dott.ssa Depaoli Francesca;
- a partire dal 1 luglio 2021, la notificazione di una violazione di dati personali deve essere inviata al Garante non più attraverso apposito modello, come indicato all'art. 6 della procedura adottata dal Comune, ma tramite una apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità.

Ritenuto necessario aggiornare la procedura approvata con deliberazione giuntale n.164/2018, adeguando le disposizioni dei seguenti articoli:

- all'art. 4 inserendo il nominativo del Referente Privacy e Data Breach;
- all'art. 5 eliminando il riferimento al Gruppo di Gestione delle violazioni, che non è stato istituito presso l'ente;
- all'art. 6 aggiornando le modalità di segnalazione al Garante della Privacy da effettuarsi non più con apposito modello, ma attraverso l'apposita procedura telematica disponibile sul portale dei servizi dell'Autorità.

Esaminata la proposta e ritenutala meritevole di approvazione in quanto rispondente alle finalità e contenuti previsti dagli 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 e ss.mm.;
- il Regolamento (UE) 2016/679, e in particolare gli artt. 33 e 34;
- il D.Lgs. 10.08.2018 n. 101;
- il Regolamento per la disciplina dei controlli interni, approvato con deliberazione consiliare n. 50 del 28.12.2016 e di questi in particolare il Capo II – Controlli di regolarità amministrativa e contabile;
- lo Statuto comunale;

Vista la deliberazione consiliare di Imer n. 32 del 19.12.2024 con la quale è stato approvato DUP semplificato 2025/2027, il Bilancio di previsione 2025/2027 e la nota integrativa al bilancio di previsione finanziario 2025/2027.

Richiamata la deliberazione della Giunta comunale di Imer n. 1 del 09.01.2025 con la quale è stato approvato il P.E.G. finanziario 2025-2027.

Vista la deliberazione giuntale n. 42 dd. 27.03.2025 con la quale è stato approvato il PIAO 2025-2027.

Dato atto che in relazione al presente provvedimento non sono state segnalate situazioni di conflitto di interesse, anche potenziale, dai dipendenti che hanno preso parte all'istruttoria.

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.

Ritenuto di dichiarare la presente deliberazione immediatamente eseguibile ai sensi e per gli effetti di cui all'art. 183, comma 4, della L.R. 03.05.2018, n. 2, stante la necessità di rendere la procedura operativa il prima possibile.

Con voti favorevoli unanimi espressi nelle forme di legge, anche avuto riguardo all'immediata eseguibilità da conferire al presente provvedimento;

DELIBERA

1. Che le premesse formano parte integrante e sostanziale del presente atto.
2. Di aggiornare la procedura per la gestione delle violazioni dei dati personali "Data Breach", ai sensi del Regolamento (UE) 2016/2018, approvata con precedente deliberazione giuntale n. 164/2018, introducendo le seguenti modifiche:
   - all'art. 4 inserendo il nominativo del Referente Privacy e Data Breach;
   - all'art. 5 eliminando il riferimento al Gruppo di Gestione delle violazioni, che non è istituito presso l'ente;
   - all'art. 6 aggiornando le modalità di segnalazione al Garante della Privacy da effettuarsi non più con apposito modello, ma attraverso l'apposita procedura telematica disponibile sul portale dei servizi dell'Autorità,

   confermando i restanti contenuti della procedura approvata con il citato Atto.
3. Di dare atto che il presente provvedimento sarà trasmesso a tutto il personale dipendente e agli Amministratori del Comune di Imèr.
4. Di comunicare, contestualmente alla pubblicazione all'Albo telematico, la presente deliberazione ai Capigruppo consigliari, ai sensi dell'art. 183 del Codice degli Enti locali approvato con L.R. 03.05.2018, n. 2.
5. Di dichiarare il presente provvedimento immediatamente eseguibile, con separata votazione favorevole all'unanimità ai sensi dell'art. 183, comma 4, del nuovo Codice degli Enti Locali della Regione Trentino Alto-Adige approvato con L.R. 3 maggio 2018, n. 2 e ss.mm., stante la necessità di rendere la procedura operativa il prima possibile.
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
Gubert Daniele	Depaoli dott.ssa Francesca

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 IMÈR

Provincia di Trento

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

Documento approvato con Deliberazione giuntale n. 164 di data 20.12.2018

Documento modificato con Deliberazione giuntale n.124 di data 22.10.2025

INDICE

1 SCOPO 2
2 AGGIORNAMENTO 2
3 DEFINIZIONI 2
4 ORGANIZZAZIONE DELLE ATTIVITÀ DI GESTIONE DELL'EVENTO VIOLAZIONE DEI DATI PERSONALI 2
5 GESTIONE DELLE ATTIVITÀ CONSEGUENTI AD UNA POSSIBILE VIOLAZIONE DI DATI PERSONALI 3
6 NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ GARANTE 3
7 COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI AGLI INTERESSATI 3
8 COMPILAZIONE DEL REGISTRO DELLE VIOLAZIONI DEI DATI PERSONALI 4

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

Con atto prot. n. 1939 dd. 29.04.2024 il Titolare ha provveduto a designare il Referente della gestione delle violazioni dei dati personali (di seguito Referente data breach), nella figura del Segretario comunale Depaoli Francesca.
Con nota prot. n. 4254 dd. 24.09.2025 è stata inviata specifica informativa ai dipendenti, comunicando nel contempo il nome del Designato.
Avvalendosi del Referente data breach, è stato predisposto 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 Protezioni Dati.
- 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 al 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 del 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.