COMUNE DI RONCHI VALSUGANA

PROVI NCI A DI TRENTO

Verbale di deliberazione N. 26

della Giunta comunale

OGGETTO: **Artt. 33 e 34 del Regolamento (UE) 2016/679. Aggiornamento della procedura per la gestione delle violazioni dei dati personali ("data breach").**

L'anno **DUEMILAVENTISEI** addì **ventisei** del mese di **marzo**, alle ore 19.00, Solita sala delle Adunanze, a seguito di regolari avvisi, recapitati a termine di legge, si è convocata la Giunta comunale.

.

Presenti i signori:

1. Ganarin Federico Maria - Sindaco
2. Caumo Alessandro - Vicesindaco
3. Debortoli Francesca - Assessore
4. Casagranda Nicola - Assessore

Assenti	
giust.	ingiust.

Assiste il Segretario Comunale Campaldini dott.ssa Alessia.

Riconosciuto legale il numero degli intervenuti, il Signor Ganarin Federico Maria, 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. Aggiornamento della procedura per la gestione delle violazioni dei dati personali ("data breach").

LA GIUNTA COMUNALE

Dato atto che è stato acquisito il preventivo parere di regolarità tecnica, espresso in modo favorevole dal Segretario comunale ai sensi dell'art. 185 del Codice degli Enti locali della Regione Trentino Alto Adige approvato con L.R. 03.05.2018, n. 2;

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);
• 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", 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 questo comune ha ritenuto di avvalersi della facoltà – prevista dall'art. 37, paragrafo 3, del Regolamento (UE) 2016/679 – di procedere alla designazione condivisa di uno stesso RPD con altri enti locali della Provincia Autonoma di Trento, sulla base delle valutazioni condotte di concerto con i predetti enti in ordine alle dimensioni della propria struttura organizzativa, all'affinità tra le rispettive strutture organizzative, le funzioni esercitate ed i trattamenti di dati personali effettuati nonché nel rispetto del principio di economicità e razionalizzazione della spesa.

Rilevato, a tal proposito, che:
- con deliberazione della giunta comunale n. 27 di data 18.04.2018, è stato affidato al Consorzio dei Comuni Trentini s.c.a.r.l. il "Servizio Responsabile della protezione dei dati personali (RPD)" nel rispetto della vigente normativa, in quanto società in house providing, incarico rinnovato poi negli anni successivi;
- con successiva nota è stato designato il Consorzio dei Comuni Trentini s.c.a.r.l., nella persona del dott. Gianni Festi – coordinatore dello staff del Servizio Responsabile della protezione dei dati personali (RPD) – quale Responsabile della protezione dei dati del comune di cui all'art. 37 del Regolamento (UE) 2016/679.
- con deliberazione della Giunta comunale n. 6 dd. 08.02.2024 il nominativo del dott. Gianni Festi è stato sostituito con la nuova referente per il Consorzio dei Comuni trentini – Responsabile della protezione dati per il Comune di Torcegno - dott.ssa Laura Marinelli;

Sottolineato come questo comune 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").

Preso atto che il Servizio segreteria di questo comune, con il supporto del Servizio Responsabile della protezione dei dati personali (RPD) svolto dal Consorzio dei Comuni Trentini s.c.a.r.l., ha elaborato a tal fine, una proposta di procedura disciplinante la gestione delle violazioni dei dati personali ("data breach").

Verificato come la procedura in oggetto risulti comprensiva dei segueti allegati:
• flusso degli adempimenti in caso di violazione dei dati personali;
• modello di potenziale violazione dei dati personali al Responsabile Protezione Dati;
• modello comunicazione violazione all'Autorità Garante.

Vista la deliberazione della Giunta comunale n. 20 dd. 21.02.2019 avente ad oggetto : "Artt. 33 e 34 del Regolamento (UE) 2016/679. Adozione della procedura per la gestione delle violazioni dei dati personali ("data breach");

Dato atto che in seguito all'ultimo audit 2025 con il Servizio RPD – Consorzio dei Comuni trentini, è stato suggerito un aggiornamento della procedura di Data Breach in quanto la precedente versione recava riferimenti al Gruppo di gestione delle violazioni – all'art. 5 – che non è operante all'interno del Comune e recava riferimenti non più attuali per la notifica al Garante che adesso può essere svolta tramite sito ufficiale del Garante per la protezione dei dati personali; Inoltre è stata indicata nel Segretario comunale la persona referente Data Breach dell'Ente;

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

Ricordato che il Sindaco, nella sua qualità di Titolare del trattamento, ha nominato nella persona del Segretario comunale il Referente della gestione delle violazioni dei dati personali ("Referente data breach");

Vista la Legge Regionale 29.10.2014 n. 10, 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 06.11.2012 n. 190 e dal D.Lgs.14.03.2013 n. 33.

Visti:
- il "Codice degli enti Locali della Regione Autonoma TAA" approvato con Legge Regionale del 03 maggio 2018 n. 2 e ss.mm.
- la legge provinciale 19 luglio 1990, n. 23 e s.m.;
- la legge provinciale n. 2 del 9 marzo 2016 e s.m.i.;
- il vigente Regolamento di contabilità;
- il D. Lgs. 23 giugno 2011 n. 118 e s.m.;
- il D. Lgs. 18 agosto 2000 n. 267 (Testo Unico Enti Locali) e s.m.i.;
- il Codice in materia di protezione dei dati personali di cui al D.Lgs. 30.06.2003 n. 196;
- il Regolamento (UE) 2016/679 del parlamento Europeo e del Consiglio d.d. 27.04.2016;
- lo Statuto Comunale vigente;

con voti unanimi favorevoli espressi in forma palese;

DELIBERA

1. di aggiornare, per le motivazioni esposte in premessa, la procedura disciplinante la gestione delle violazioni dei dati personali ("data breach") di cui agli artt. 33 e 34 del Regolamento (UE) 2016/679, allegata alla presente deliberazione per formarne parte integrante e sostanziale;

2. di evidenziare che la procedura di cui al precedente punto 1) risulta comprensiva dei seguenti allegati:
- flusso degli adempimenti in caso di violazione dei dati personali;

- modello di potenziale violazione dei dati personali al Responsabile Protezione Dati;
- modello comunicazione al Referente;

3. di stabilire che verrà istituito apposito registro delle violazioni;

4. di dare atto che il presente provvedimento va pubblicato sul sito istituzionale di questo Ente e ad essa va data ulteriore pubblicità, quale condizione integrativa d'efficacia, per un periodo di 5 anni, ai sensi della L.R. 29.10.2014 n. 10, nei casi previsti dal Decreto Legislativo n. 33 del 14 marzo 2013 e dalla Legge 6 novembre 2012, n. 190;

5. di dare atto che il Sindaco, nella sua qualità di Titolare del trattamento, ha designato quale Referente della gestione delle violazioni dei dati personali ("Referente data breach") il Segretario comunale;

6. di trasmettere copia della presente deliberazione al personale dipendente;

Ai sensi dell'art. 4, comma 4, della L.P. 23/92 e ss.mm., avverso la presente deliberazione sono ammessi i seguenti ricorsi:

a) opposizione alla Giunta comunale durante il periodo di pubblicazione ai sensi dell'art. 183, comma 5, vigente Codice degli Enti Locali della Regione Trentino Alto Adige approvato con L.R. 03/05/2018 n°2;

b) ricorso giurisdizionale al T.R.G.A. di Trento, entro 60 giorni, ai sensi degli artt. 13 e 29 del D.Lgs. 02.07.2010, n. 104;

c) in alternativa, ricorso straordinario al Presidente della Repubblica, entro 120 giorni, ai sensi dell'art. 8 del D.P.R. 24.11.1971, n. 1199.

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

IL SINDACO	IL SEGRETARIO COMUNALE
Ganarin Federico Maria	Campaldini dott.ssa Alessia

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).

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

Documento approvato con Delibera di data		
Revisione	Data	Motivo
Prima	Marzo 2026	Aggiornamento con riferimenti attuali alla normativa

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 e che l'Ente ha individuato nella persona del Segretario comunale.
- 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.

Esempi di Data breach tratti dalle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE 279/2016

	Violazione	Tipologia di violazione			Note/raccomandazioni
		Disponibilità	Riservatezza	Integrità	
1	Un addetto dell'ente smarrisce o subisce il furto di un dispositivo di memorizzazione (cd, dvd, hd esterno, pen drive) o di un dispositivo personale (pc, tablet, smartphone) contenenti dati personali non protetti da crittografazione e non recuperabili dalle copie di backup.	X	X		Nel caso in cui i dati siano crittografati l'evento non è da considerare una violazione della riservatezza. Nel caso in cui siano disponibili copie di backup l'evento non è da considerare una violazione della disponibilità.
2	A causa di un malware o di un virus informatico l'ente perde l'unica copia non recuperabile dal backup di un insieme di dati personali (database o cartelle).	X	X		
3	A causa di un evento dannoso quale può essere un incendio o un allagamento l'ente perde alcune banche dati (originali cartacee o elettroniche senza possibilità di ripristino dalle copie di backup).	X			
4	Il locale archivio dell'ente subisce una effrazione e il furto di alcuni faldoni contenenti dati personali.	X	X		
5	Documenti contenenti dati personali sono stati smaltiti per errore in un cestino gettacarte anziché essere distrutti in modo sicuro. Il cestino è stato svuotato in un bidone lasciato all'esterno dell'ufficio ai fini della raccolta dei rifiuti. Un terzo ha prelevato la busta da quest'ultimo bidone e ha avuto accesso ai dati personali.		X		
6	A seguito di un attacco informatico ad un servizio online dell'ente vengono prelevati e diffusi dati personali degli utenti.	X	X		
7	Un dipendente ha rivelato ad un terzo il login e la password di un account con privilegi di accesso completo ad una o più basi dati dell'ente. Utilizzando tale account, il terzo può accedere a tutte le informazioni presenti nella base dati quali nomi, indirizzi, indirizzi di posta elettronica, numeri di telefono, dati di accesso e altri dati di identificazione (nome utente, hash delle password, ID dei clienti).		X	X	
8	A seguito di un guasto, di una interruzione di corrente o della connettività si verifica una prolungata sospensione nell'erogazione dei servizi ai cittadini.	X			
9	Un cittadino segnala di aver ricevuto per sbaglio documentazione contenente dati personali relativi ad altri soggetti.		X		
10	Una e-mail contenente dati personali viene inviata per sbaglio ad un elevato numero di destinatari.		X		

COMUNE DI TORCEGNO

PROVINCIA DI TRENTO

C.A.P. 38050 - ☎ (0461) 760777

e-mail:

sindaco@comunetorcegno.it

comune@pec.comune.torcegno.tn.it

Cod. Fisc. e P. IVA 00291650224

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 _____