ORIGINALE

COMUNE DI TELVE DI SOPRA

(Provincia di Trento)

Verbale di deliberazione N. 96

della Giunta comunale

OGGETTO: **Approvazione dello schema di procedura per la gestione della violazione dei dati personali (DATA BREACH) del Comune di Telve di Sopra.**

L'anno **DUEMILADICIOTTO** addì **ventisette** del mese di **novembre**, alle ore 11.30, nella sala delle riunioni, formalmente convocato si è riunita la Giunta comunale.

Presenti i signori:

1. Colme Ivano - Sindaco
2. Trentin Sara - Vicesindaco
3. Trentin Martino - Assessore

Assenti	
giust.	ingiust.

Assiste il Segretario Comunale Signora Iuni dott.ssa Silvana.

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

Premesso:

- la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale;
- l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea ("Carta") e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione Europea ("TFUE") stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;
- il Parlamento Europeo e il consiglio dell'Unione Europea hanno approvato il 27 aprile 2016 il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, abrogando la Direttiva 95/46/CE (di seguito solo "GDPR");
- il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;
- il Regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi, effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione;
- in esecuzione del GDPR ed al fine di attuare un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, è richiesto alle aziende e alle Pubbliche Amministrazioni di approntare un piano di protezione dei dati personali che, partendo dalla mappatura e dall'analisi dei trattamenti, effettui la valutazione del rischio di violazione ed individui infine le misure volte ad eliminare o almeno ridurre il rischio stesso;
- dato atto che permane comunque la possibilità che i dati personali vengano violati da parte di soggetti terzi, e che si rende quindi necessario prevedere una procedura da attuare nel caso si verificasse l'evento in questione

LA GIUNTA COMUNALE

Visto lo schema di procedura per la gestione della violazione dei dati personali (DATA BREACH) predisposto dal Consorzio dei Comuni, con sede a Trento in via Torre Verde, 23, in qualità di Responsabile della Protezione dei dati del Comune di Telve di Sopra, che 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;

Visti gli allegati allo schema di cui sopra, ed in particolare:

- Allegato A: potenziale violazione di dati personali - modello di comunicazione al responsabile della protezione dei dati;
- Allegato B: violazione di dati personali - modello di comunicazione al garante;

Ritenuto il predetto schema, con i relativi allegati, meritevole di approvazione;

Visto il Regolamento UE n. 679/2016;

Viste le indicazioni fornite dall'Autorità Garante per la Protezione dei Dati personali e dal Responsabile Protezione Dati del Comune di Telve di Sopra;

Visto il Codice Enti Locali della Regione Autonoma Trentino Alto Adige, approvato con L.R. 3.05.2018 n. 2 e s.m.;

Visto il parere espresso ai sensi dell'art. 185 del Codice Enti Locali, approvato con L.R. 3.05.2018 n. 2, sulla presente proposta di deliberazione:

- dal Segretario Comunale in ordine alla regolarità tecnico-amministrativa espresso in data 19 novembre 2018;

Dato atto che il presente provvedimento non necessita del parere di regolarità contabile di cui all'art. agli artt. 185 e 187 del Codice Enti Locali, approvato con L.R. 3.05.2018 n. 2 in quanto non comporta impegni di spesa o diminuzioni di entrate;

Accertata la propria competenza

Ad unanimità di voti espressi per alzata di mano

DELIBERA

1. di approvare lo schema di procedura per la gestione della violazione dei dati personali (DATA BREACH), così come predisposto dal Consorzio dei Comuni, con sede a Trento in via Torre Verde, 23, in qualità di Responsabile della Protezione dei dati del Comune di Telve di Sopra, che 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, ivi compresi i relativi allegati "A" e "B", che allegato alla presente deliberazione ne costituisce parte integrante e sostanziale;

2. di disporre che tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali dell'Ente vengano informati del presente provvedimento e osservino la presente Procedura;

3. di trasmettere la presente deliberazione ai capigruppo consiliari ai sensi e per gli effetti del disposto dell'art. 183 comma 2 della L.R. 03 maggio 2018 nr. 02;

4. di dare atto che la presente deliberazione diverrà esecutiva dopo la pubblicazione all'albo pretorio ai sensi dell'art. 183, terzo comma, del Codice Enti Locali, approvato con L.R. 03 maggio 2018 nr. 02.

Ai sensi dell'articolo 4 della Legge provinciale 30 novembre 1992, n. 23, avverso il presente provvedimento sono ammessi i seguenti ricorsi:
a) opposizione alla Giunta comunale entro il periodo di pubblicazione, ai sensi dell'art. 183, comma 5, della Legge Regionale 3 maggio 2018, n. 2;

b) ricorso al Tribunale amministrativo regionale di Trento entro 60 giorni, ai sensi dell'art. 29 del D.Lgs. 2 luglio 2010, n. 104;
c) ricorso straordinario al Presidente della Repubblica entro 120 giorni, ai sensi dell'art. 8 del D.P.R. 24 novembre 1971, n. 1199.
I ricorsi b) e c) sono alternativi

In materia di aggiudicazione di appalti si richiama la tutela processuale di cui al comma 5) dell'art. 120 dell'Allegato 1) al D.Lgs. 02 luglio 2010 n. 104. In particolare:
- il termine per il ricorso al Tribunale Amministrativo Regionale è di 30 giorni; - non è ammesso il ricorso sub c)

Letto, approvato e sottoscritto.

IL SINDACO	IL SEGRETARIO COMUNALE
Colme Ivano	Iuni dott.ssa Silvana

Il presente verbale è stato pubblicato all'Albo comunale il 03/12/2018 per rimanervi per dieci giorni consecutivi. Contestualmente all'affissione all'albo la presente deliberazione è stata comunicata ai capigruppo consigliari, ai sensi dell'art. 79, comma 2 del Testo Unico delle Leggi Regionali sull'ordinamento dei comuni della Regione Autonoma Trentino-Alto Adige approvato con D.P.Reg. 01.02.2005, n. 3/L e s.m.

IL SEGRETARIO COMUNALE

Iuni dott.ssa Silvana

La presente deliberazione è stata pubblicata all'albo comunale per dieci giorni consecutivi fino al 13/12/2018 e nel corso del periodo di pubblicazione non sono pervenute opposizioni.

Telve di sopra, lì 14/12/2018

IL SEGRETARIO COMUNALE

Iuni dott.ssa Silvana

La presente deliberazione è divenuta esecutiva il giorno 14 dicembre 2018 ai sensi dell'art. 79, comma 3 del Testo Unico delle Leggi Regionali sull'ordinamento dei comuni della Regione Autonoma Trentino-Alto Adige approvato con D.P.Reg. 01.02.2005, n. 3/L e s.m.

IL SEGRETARIO COMUNALE

Iuni dott.ssa Silvana

COMUNE DI TELVE DI SOPRA

Provincia di Trento
Via S. Giovanni Bosco, 10
38050 TELVE DI SOPRA (TN)
telefono: 0461 766001 - fax 0461 760793
C.F. 81001210228 - P. IVA 00390750222
e-mail: info@comune.telvedisopra.tn.it
pec: comune@pec.comune.telvedisopra.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 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.) attraverso la compilazione del "Modello di potenziale violazione di dati personali al Responsabile Protezione Dati" – allegato "A";
- 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.

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 avvalendosi del "Modello comunicazione violazione all'Autorità Garante" – allegato "B".
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.

COMUNE DI TELVE DI SOPRA

Provincia di Trento
Via S. Giovanni Bosco, 10
38050 TELVE DI SOPRA (TN)
telefono: 0461 766001 - fax 0461 760793
C.F. 81001210228 - P. IVA 00390750222
e-mail: info@comune.telvedisopra.tn.it
pec: comune@pec.comune.telvedisopra.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 _____

COMUNE DI TELVE DI SOPRA

Provincia di Trento
Via S. Giovanni Bosco, 10
38050 TELVE DI SOPRA (TN)
telefono: 0461 766001 - fax 0461 760793
C.F. 81001210228 - P. IVA 00390750222
e-mail: info@comune.telvedisopra.tn.it
pec: comune@pec.comune.telvedisopra.tn.it

VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dall'articolo ART 33 del GDPR, il Titolare è tenuto a comunicare all'Autorità Garante per la protezione dei dati personali all'indirizzo protocollo@pec.gpdp.it le violazioni dei dati personali (*data breach*) di cui è titolare.

La comunicazione deve essere effettuata entro 72 ore dalla conoscenza del fatto.

L'Ente titolare del trattamento

Denominazione o ragione sociale _____

Provincia Trento, Comune _____

Cap _____ Indirizzo _____

Nome e Cognome della persona fisica addetta alla comunicazione _____

Funzione rivestita _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

Eventuali contatti (altre informazioni) _____

Nome e dati contatto RPD _____

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 oggetto della violazione

- ☐ Computer
- ☐ Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di backup
- ☐ Documento cartaceo
- ☐ Altro_____

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

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 _____

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

- ☐ Basso/trascurabile
- ☐ Medio
- ☐ Alto
- ☐ Molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione

La violazione è stata comunicata anche agli interessati?

- ☐ Sì, è stata comunicata il
- ☐ No, perché _____

Qual è il contenuto della comunicazione resa agli interessati?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?