COMUNE DI CAMPODENNO

PROVINCIA DI TRENTO

VERBALE DI DELIBERAZIONE N. 19/2020
DELLA GIUNTA COMUNALE

OGGETTO: **ARTT. 33 E 34 DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (UE) 2016/679. APPROVAZIONE SCHEMA DI PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH).**

L'anno **duemilaventi** addì **diciotto** del mese di **febbraio** alle ore **17.30** nella sala delle riunioni, presso la sede Municipale di Campodenno, la Giunta Comunale di questo Comune si è radunata sotto la presidenza del Sindaco sig. Biada Daniele.

All'appello risultano i signori:

		Assenti	
		giustificati	Ingiustificati
BIADA DANIELE	Sindaco		
PEDO' OSCAR	Assessore - Vicesindaco		
CATTANI GIOVANNA	Assessore		
PORTOLAN IGOR	Assessore		
BERTOLAS GIANLUCA	Assessore		

Assiste il Segretario comunale dott.ssa Ivana Battaini.

Riconosciuto legale il numero degli intervenuti, il signor BIADA DANIELE nella sua qualità di Sindaco dichiara aperta la seduta, dando atto che è stata osservata la procedura istruttoria, invita quindi i presenti a prendere in esame e deliberare in merito all'argomento in oggetto indicato.

LA GIUNTA COMUNALE

Premesso che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale;

Considerato che il 25 maggio 2016 è entrato in vigore il Regolamento Europeo Privacy UE/2016/679 o GDPR (General Data Protection Regulation) che stabilisce le nuove norme in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché le norme relative alla libera circolazione di tali dati;

Rilevato che il summenzionato Regolamento è direttamente applicabile in ciascuno degli Stati membri dell'Unione Europea ed entrerà in vigore il 25 maggio 2018;

Considerato che con il Regolamento Europeo Privacy UE/2016/679 viene recepito nel nostro ordinamento giuridico il "principio di accountability" (obbligo di responsabilizzazione) che impone alle Pubbliche Amministrazioni titolari del trattamento dei dati: - di dimostrare di avere adottato le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche; - che i trattamenti siano conformi ai principi e alle disposizioni del Regolamento, prevedendo, altresì, l'obbligo del titolare o del responsabile del trattamento della tenuta di apposito registro delle attività di trattamento, compresa la descrizione circa l'efficacia delle misure di sicurezza adottate; - che il registro di cui al punto precedente, da tenersi in forma scritta - o anche in formato elettronico, deve contenere una descrizione generale delle misure di sicurezza tecniche e organizzative e che su richiesta, il titolare del trattamento o il responsabile del trattamento sono tenuti a mettere il registro a disposizione dell'autorità di controllo;

Tenuto conto, inoltre, che il Regolamento Europeo Privacy UE/2016/679 ha: - disciplinato la nuova figura del "Data Protection Officer" (DPO), responsabile della protezione dei dati personali che le pubbliche amministrazioni hanno l'obbligo di nominare al proprio interno e deve sempre essere "coinvolto in tutte le questioni riguardanti la protezione dei dati personali"; - rafforzato i poteri delle Autorità Garanti nazionali ed inasprito le sanzioni amministrative a carico di imprese e pubbliche amministrazioni, in particolare, in caso di violazioni dei principi e disposizioni del Regolamento, le sanzioni possono arrivare fino a 10 milioni di euro o per le imprese fino al 2% - 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore;

Rilevato che gli articoli 33 e 34 del Regolamento UE si soffermano in particolare sul tema della violazione dei dati e sulla procedura ad adottare in caso di "data breach", disponendo che il soggetto che viene a conoscenza di una possibile violazione dei dati personali deve immediatamente darne segnalazione al referente privacy dell'Ente ed al Referente Data Breach, i quali successivamente adotteranno le misure adeguate per porre rimedio alla violazione, informando il Responsabile Protezione dati il quale valuterà la necessità di notificare l'evento al Garante della Privacy;

Dato atto che la nuova normativa europea fa carico alle Pubbliche Amministrazioni di non limitarsi alla semplice osservanza di un mero adempimento formale in materia di privacy, conservazione e sicurezza dei dati personali, ma attua un profondo mutamento culturale e concettuale con un rilevante impatto organizzativo da parte dell'Ente nell'ottica di adeguare le norme di protezione dei dati ai cambiamenti determinati dalla continua evoluzione delle tecnologie (cloud computing, digitalizzazione, social media, cooperazione applicativa, interconnessione di banche dati, pubblicazione automatizzata di dati on line) nelle amministrazioni pubbliche;

Considerato 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.

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 n. 23, in qualità di Responsabile della Protezione dei dati del Comune di Campodennonore, 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 dell'interessato, in ossequio alle previsioni di cui agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016;

Verificato che a tal proposito il Comune di Campodenno con determinazione del Segretario comunale n. 19 di data 18.04.2018 ha affidato al Consorzio dei Comuni Trentini, in quanto società in house providing, il "Servizio di Responsabile della protezione dei dati personali (RPD)" nel rispetto della vigente normativa. Inoltre il riferimento della designazione obbligatoria del RDP, il Titolare con atto prot. numero

1676 di data 17.05.2018 ha designato il Consorzio dei Comuni Trentini, nella persona del dott. Gianni Festi coordinatore dello staff del Servizio Responsabile della protezione dei dati personali (RDP)- quale Responsabile della Protezione dei dati dell'Ente;

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 Campodenno;

Dato atto che l'adozione del presente provvedimento non comporta impegno di spesa e, pertanto, non risulta necessario alcun parere in ordine alla regolarità contabile del provvedimento amministrativo;

Acquisito il parere favorevole in ordine alla regolarità tecnica, espresso dal Segretario comunale ai sensi dell'articolo 185 della L.R. 03.05.2018 n. 2;

Visti:

- Il Codice degli Enti Locali della regione Autonoma Trentino Alto Adige approvato con legge Regionale del 03.05.2018 n. 2 con particolare riferimento all'articolo 126 relativo alla figura dei dirigenti ed alle competenze loro attribuite;
- il Regolamento di attuazione dell'Ordinamento finanziario e contabile degli enti locali approvato con DPGR 27.10.1999 n. 8/L;
- lo Statuto Comunale approvato con deliberazione consiliare n. 13 di data 31.03.2009 e da ultimo modificato con deliberazione consiliare n. 11 di data 09.04.2019;

Ad unanimità di voti palesemente espressi per alzata di mano;

D E L I B E R A

1. Di approvare lo schema di procedura per gestione della violazione dei dati personali (DATA BREACH), così come predisposto dal Consorzio dei Comuni, con sede a Trento in via Torre Verde n. 23, in qualità di Responsabile della Protezione dei dati del Comune di Campodenno, 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 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 allegati 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 dare atto che la presente deliberazione diventa esecutiva a pubblicazione avvenuta ai sensi del comma 3 dell'art. 183 della L.R. 03.05.2018 n. 2;
4. Di inviare, contestualmente all'affissione all'Albo Pretorio, copia della presente deliberazione ai capigruppo consiliari ai sensi e per gli effetti dell'art. 183, comma 2, della L.R. 03.05.2018 n. 2.
5. Di dare atto che avverso la presente deliberazione sono ammessi i seguenti mezzi di impugnativa:
   - opposizione alla Giunta Comunale, entro il periodo di pubblicazione, ai sensi dell'art. 183 comma 5 della L.R. 03.05.2018 n. 2;
   - ricorso giurisdizionale al T.R.G.A. di Trento, entro il termine di 60 giorni, ai sensi dell'art. 29 del D. Lgs. 02.07.2010 n. 104;
   - ricorso straordinario al Presidente della Repubblica, entro il termine di 120 giorni, ai sensi dell'art. 8 del D.P.R. 24.11.1971 n. 1199.

Data lettura del presente verbale, viene approvato e sottoscritto

IL SINDACO	IL SEGRETARIO COMUNALE
Daniele Biada	Dott.ssa Ivana Battaini
Documento informatico firmato digitalmente ai sensi e con gli effetti di cui agli artt. 20 e 21 del D. Lgs n. 82/2005, sostituisce il documento cartaceo e la firma autografa.	*Documento informatico firmato digitalmente ai sensi e con gli effetti di cui agli artt. 20 e 21 del D. Lgs n. 82/2005, sostituisce il documento cartaceo e la firma autografa.*