COMUNE DI SAGRON MIS

PROVINCIA DI TRENTO

Verbale di deliberazione N. 52

della Giunta comunale

OGGETTO: **Artt.33 e 34 del Regolamento (UE) 2016/679. Approvazione procedura per la gestione delle violazioni dei dati personali "Data Breach".**

L'anno **DUEMILAVENTIDUE** addì **undici** del mese di **agosto**, alle ore 16.00, nella sala delle riunioni, a seguito di regolari avvisi, recapitati a termine di legge, si è convocata la Giunta comunale.

Presenti i signori:

1. Depaoli Marco - Sindaco
2. Broch Annalisa - Vicesindaco
3. Daldon Elio - Assessore
4. Marcon Oriano - Assessore

Assenti	
giust.	ingiust.

Assiste il Segretario Comunale Serafini Samuel.

Riconosciuto legale il numero degli intervenuti, il Signor Depaoli Marco, 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. Approvazione procedura per la gestione delle violazioni dei dati personali "Data Breach".

LA GIUNTA COMUNALE

Premesso che :

- il 25 maggio 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 che ha abrogato 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.

Atteso che il Regolamento (UE) 2016/679 – denominato "Regolamento generale sulla protezione dei dati" – detta una nuova disciplina in materia di trattamento dei dati personali, prevedendo in particolare un nuovo elemento innovativo quale il "principio di responsabilizzazione" (c.d. accountability") che pone al centro del nuovo quadro normativo la figura del "Responsabile della protezione dei dati" – RPD.

Rilevato che il Comune di Sagron Mis 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 gli altri Enti locali della Provincia autonoma di Trento, tenuto conto delle valutazioni condotte in accordo con gli altri Enti in ordine alla propria struttura organizzativa, alla similitudine tra le rispettive strutture, alle funzioni esercitate e i trattamenti di dati personali effettuati nonché tenuto conto del principio dell'efficacia ed efficienza nonché della razionalizzazione della spesa.

Considerato che :

- con deliberazione giuntale n. 59, dd. 29.05.2018, è stato affidato al Consorzio dei Comuni Trentini s.c.ar.l. l'incarico per il "Servizio Responsabile della protezione dei dati personali (RPD) nel rispetto della normativa vigente in quanto società "in house" providing;
- con il medesimo provvedimento è stato disposto di 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 della medesima Comunità come statuito art. 37 del Regolamento succitato.

Rilevato che tra gli adempimenti previsti rientri quello previsto agli artt.33 e 34 del Regolamento (UE) 2016/679 e precisamente quello attinente all'adozione di una specifica procedura che disciplini la gestione delle violazioni dei dati personali (data breach).

Considerato che in attesa dell'adozione di specifica procedura l'Ente si è comunque tempestivamente attivato per informare il personale e gli amministratori dell'Ente di segnalare tempestivamente al referente della privacy dell'Ente e al Segretario nel caso fossero rilevate violazioni dei dati personali al fine di adottare gli adempimenti di competenza.

Preso atto peraltro che in proposito la segreteria del Comune con il supporto del Consorzio dei Comuni Trentini nella figura del Responsabile della protezione dei dati personali (RPD) ha elaborato una proposta di procedura disciplinante la gestione delle violazioni dei dati personali (data breach).

Dato atto che la procedura in argomento è comprensiva dei seguenti allegati ;

- Registro delle violazioni dei dati personali;
- Flusso degli adempimenti in caso di violazione dei dati personali;
- Modello comunicazione potenziale violazione al RPD;
- Modello di comunicazione della violazione all'Autorità Garante.

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.

Considerato altresì che compete al Sindaco designare il Referente della gestione delle violazioni dei dati personali ("Referente data breach").

Visti:

- il Codice degli Enti Locali della Regione Autonoma Trentino Alto Adige, approvato con Legge Regionale 03.05.2018, n. 2 come modificato con Legge Regionale 08.08.2018, n.6 e dalla Legge Regionale 01.08.2019, n. 3;
- la Legge Provinciale 09.12.2015, n. 18 "Modificazioni della legge di contabilità 1979 e altre disposizioni di adeguamento all'ordinamento provinciale e degli enti locali al D.Lgs. 118/2011 e s.m. (disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle regioni, degli enti locali e dei loro organismi, a norma degli artt. 1 e 2 della Legge 05.05.2009, n. 42);
- il Testo Unico delle Leggi sull'Ordinamento degli Enti Locali approvato con D.Lgs. 18.08.2000, n 267 e ss.mm.;
- il Regolamento di contabilità, approvato con deliberazione consiliare n. 8, del 26.03.2018;
- le convenzioni per la gestione in forma associata dei servizi finanziario – Tecnico – Urbanistica e Segreteria sottoscritte dal Comune di Sagron Mis con i Comuni di Mezzano e Imer e la Comunità di Primiero.

Vista la deliberazione consiliare n. 34, dd. 21.12.2021, con la quale è stato approvato il Documento Unico di Programmazione 2022/2024, del bilancio di previsione finanziario 2022/2024 e della nota integrativa al bilancio medesimo.

Dato atto che non sussistono situazioni di conflitto di interesse in capo ai responsabili dell'istruttoria di questo provvedimento ai sensi dell'articolo 7 del Codice di comportamento dei dipendenti del Comune di Sagron Mis.

Acquisito altresì dal Segretario comunale il parere di regolarità tecnico-amministrativa del presente atto ai sensi dell'art. 185 del CEL (Codice Enti Locali) approvato con L.R. 2/2018.

Acquisito il parere del Responsabile del Servizio Finanziario in ordine alla regolarità contabile ed alla copertura finanziaria del presente atto, per quanto di competenza, ai sensi dell'art. 185 del CEL (Codice Enti Locali) approvato con L.R. 2/2018.

Con voti unanimi favorevoli, espressi per alzata di mano

DELIBERA

1. di adottare, per le motivazioni in premessa esposte, la procedura disciplinante la gestione delle violazioni dei dati personali "data breach" di cui agli artt.33 e 34 del Regolamento (UE) 2016/679, che si allega sub 1) al presente provvedimento a formarne parte integrante e sostanziale;

2. di dare atto che la procedura di cui sopra è comprensiva dei seguenti allegati:
   - Registro delle violazioni dei dati personali;
   - Flusso degli adempimenti in caso di violazione dei dati personali;
   - Modello comunicazione potenziale violazione al RPD;
   - Modello di comunicazione della violazione all'Autorità Garante;

3. di individuare nel dipendente Comunale Claudia Loss il Referente della gestione delle violazioni dei dati personali ("Referente data breach");

4. di demandare al Segretario dell'Ente di garantire una adeguata informazione al personale dipendente dell'Ente in ordine alla procedura di cui al precedente punto 1);

5. di dare atto che il presente provvedimento diviene esecutivo a pubblicazione avvenuta;

6. di dare atto che a norma dell'art. 4, della Legge Provinciale 20.11.1992, n. 23 e ss.mm., avverso il presente provvedimento è possibile presentare:
   - opposizione alla Giunta Comunale, durante 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 dell'allegato 1) del D.Lgs. 02.07.2010, n. 104, ovvero, 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 e ss.mm..

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

IL SINDACO	IL SEGRETARIO COMUNALE
Depaoli Marco	Serafini Samuel

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).

SERVIZIO RESPONSABILE DELLA PROTEZIONE DEI DATI

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

Documento approvato con Delibera di data		
Revisione	Data	Motivo

INDICE

38050 SAGRON MIS (TN) - Via Parrocchia n. 9 - Tel. 0439 65009 - Fax 0439 652014
C.F. e P.IVA 00290910223 - Pec: comune@pec.comune.sagron-mis.tn.it

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";
- 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".
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.

SERVIZIO RESPONSABILE DELLA PROTEZIONE DEI DATI

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?