

**Verbale di Deliberazione N. 81**  
della Giunta comunale

**OGGETTO:** Adozione della procedura per la gestione delle violazioni dei dati personali (“data breach”). Articoli 33 e 34 del Regolamento (UE) 2016/679.

L'anno **DUEMILAVENTIDUE** addì **TRENTUNO**  
del mese di **MAGGIO** alle ore **18:00**

a seguito di regolari avvisi recapitati a termini di legge, si è convocata la Giunta comunale.

Presenti i signori:

Assente Giust.    Assente Ingiust.

VIELMETTI PAOLO	- Sindaco
CONFORTI FABRIZIO	- Vice Sindaco
GERVASI BARBARA	- Assessore
GERVASI GIOVANNA	- Assessore
TONIATTI GABRIELE	- Assessore

Assiste il Segretario comunale dott. Michele Rizzi

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

**OGGETTO:** Adozione della procedura per la gestione delle violazioni dei dati personali (“data breach”). Articoli 33 e 34 del Regolamento (UE) 2016/679.

**PREMESSO E RILEVATO 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 le direttive 95/46/CE (Regolamento generale sulla protezione dei dati) e rilevato inoltre che in data 19.09.2018 è entrato in vigore il D.lg. 10.08.2018 n. 101 di armonizzazione al Regolamento (UE) 2016/679.

Evidenziato come il Regolamento - denominato "Regolamento generale sulla protezione dei dati", in sigla GDPR – detti una nuova disciplina in materia del trattamento dei dati personali, e prevede tra gli elementi caratterizzanti e innovativi il "principio di responsabilizzazione" (ed. accountability) e pone al centro del nuovo quadro normativo la figura del “Responsabile della protezione dei dati” in sigla RPD.

Con determinazione della Segreteria Comunale n. 7 del 01.02.2022 si provvedeva ad affidare, al Consorzio dei Comuni Trentini con sede in Trento, il “Servizio privacy” con particolare riferimento alla figura del Responsabile della Protezione dei Dati (RPD) con durata biennale dal 01 gennaio 2022 al 31 dicembre 2023.

Il comune di Denno è tenuto, a seguito dell’entrata in vigore del Regolamento (UE) 2016/679, ad una serie di adempimenti conseguenti.

**PREMESSO QUANTO SOPRA;**

## **LA GIUNTA COMUNALE**

**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 del comune di Denno – con supporto collaborativo 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 seguenti allegati:

- Procedura per la gestione della violazione dei dati personali (data breach);
- Circolare per i dipendenti.

**ESAMINATA** la proposta di cui trattasi e ritenuta la stessa meritevole di approvazione in quanto rispondente alle finalità ad ai contenuti previsti dagli art. 33 e 34 del Regolamento (UE) 2016/679;

**STABILITO** di demandare al Sindaco, nella qualità di Titolare del trattamento, l’effettuazione della designazione del Referente della gestione delle violazioni dei dati personali (“Referente data breach”);

**RITENUTO** di dover dichiarare il presente provvedimento immediatamente eseguibile ai sensi dell’articolo 183 comma 4 del Codice degli Enti Locali della Regione autonoma Trentino – Alto Adige, approvato con L.R. 03.05.2018, n. 2, al fine di permettere l’adozione del provvedimento relativo alla procedura disciplinante la gestione delle violazioni dei dati personali;

VISTA la deliberazione consiliare n. 4 dd. 10.03.2022, immediatamente eseguibile, con la quale sono stati approvati il bilancio di previsione finanziario ed il D.U.P., per gli esercizi 2022-2024;

VISTA la deliberazione giuntale n. 19 dd. 13.04.2021 con la quale è stato approvato il P.E.G. relativo agli esercizi 2021-2023;

VISTA la deliberazione giuntale n. 28 dd. 16.03.2022 con la quale è stato approvato il P.E.G. relativo agli esercizi 2022-2024 – parte finanziaria;

VISTO lo Statuto comunale, approvato con deliberazione consiliare n. 9 dd. 30.03.2016;

VISTO il Codice degli Enti Locali della Regione Trentino Alto Adige, approvato con L.R. 03.05.2018, n. 2 e ss.mm.;

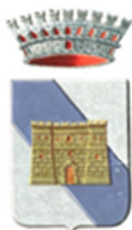
DATO ATTO che ai sensi dell'art. 185, comma 1, del Codice degli Enti locali della Regione Autonoma Trentino - Alto Adige, approvato con L.R. 03.05.2018, n. 2 sulla presente proposta di deliberazione il Segretario comunale ha espresso parere di regolarità tecnico-amministrativa;

AD unanimità di voti favorevoli, espressi per alzata di mano

## **DELIBERA**

1. di adottare, 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 formare parte integrante e sostanziale;
2. di dare atto che la procedura di cui al precedente punto 1) risulta comprensiva dei seguenti allegati:
  - o Procedura per la gestione della violazione dei dati personali (data breach)
  - o Circolare per i dipendenti
3. di incaricare il Segretario Comunale, nella sua qualità di Referente Privacy dell’ente, di garantire una adeguata informazione al personale dipendente in ordine alla procedura di cui al punto 1);
4. di dichiarare la presente, per le motivazioni espresse in premessa, immediatamente eseguibile ai sensi dell’articolo 183 comma 4 del Codice degli Enti Locali della Regione autonoma Trentino - Alto Adige, approvato con L.R. 03.05.2018 n. 2;
5. di inviare la presente ai capigruppo consiliari ai sensi dell’art. 183, comma 2, del Codice degli enti locali della Regione autonoma Trentino-Alto Adige, approvato con L.R. 03.05.2018, n. 2;
6. di dare evidenza, ai sensi dell’articolo 4 della L.P. 30.11.1992, n. 23, che avverso il presente provvedimento è ammessa:
  - opposizione alla Giunta Comunale, durante il periodo di pubblicazione, da parte di ogni cittadino ai sensi dell’articolo 183, comma 5, del Codice degli enti locali della Regione autonoma Trentino-Alto Adige, approvato con L.R. 03.05.2018 n. 2;
  - ricorso straordinario al Presidente della Repubblica entro 120 giorni ex articolo 8 del D.P.R. 24.11.1971 n. 1199;
  - ricorso giurisdizionale avanti al T.R.G.A. di Trento entro 60 giorni ex articoli 13 e 29 del D.Lgs. 02.07.2010 n. 104, da parte di chi abbia un interesse concreto ed attuale.

Ai sensi dell’articolo 183, comma 4, del Codice degli enti locali della Regione autonoma Trentino-Alto Adige, approvato con L.R. 03.05.2018, n. 2, la presente deliberazione, dichiarata immediatamente eseguibile, è pubblicata all’albo comunale, pena decadenza, entro cinque giorni dalla sua adozione per dieci giorni consecutivi.



**COMUNE DI DENNO**  
Provincia di Trento  
Via Giovanni Ossanna n. 1 – CAP 38010  
Tel 0461.655523 – Fax 0461.655549 - C.F. 80014520227  
[www.comune.denno.tn.it](http://www.comune.denno.tn.it)  
[comune@pec.comune.denno.tn.it](mailto:comune@pec.comune.denno.tn.it)



**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**

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

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 [serviziordp@comunitrentini.it](mailto:serviziordp@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.

## DATA BREACH

Riferimento normativo: articoli 33 e 34 del Regolamento UE 679/2016.  
Riferimento provvedimento: Linee guida del Gruppo “Articolo 29” in materia di notifica delle violazioni dei dati personali

### Nozione di data breach

Ai fini del data breach rilevano le violazioni di sicurezza che comportano violazione dei dati personali. Si articolano le seguenti fattispecie:

- violazioni della riservatezza ossia disvelamento o accesso indebito o accidentale ai dati personali;
- violazioni della disponibilità ossia indebito o accidentale impedimento all'accesso ai dati personali o distruzione di dati personali;
- violazione dell'integrità dei dati personali ossia indebita o accidentale alterazione dei dati personali.

### Che fare in caso di data breach

#### Gestione interna del data breach seguendo l'apposita Procedura adottata dall'Ente

In caso di supposta violazione di dati personali si avvisa tempestivamente il Referente Data breach e il Referente Privacy dell'Ente per:

- 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”;

#### Notificazione data breach al Garante

In caso di violazione dei dati personali, previo consulto con il Responsabile della Protezione dei Dati, si deve notificare la violazione al Garante per la protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

Ciò a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore è corredata dei motivi del ritardo.

La notifica deve contenere una serie di elementi come indicati nella norma, ed in particolare:

- descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- nome e dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

### **Comunicazione data breach**

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

In presenza di alcune condizioni non è necessaria la comunicazione all'interessato.

### **Registro delle violazioni**

Deve essere formato un Registro delle violazioni i dati personali.

Operativamente: nel caso si verifichi un evento che comporti o possa comportare violazione dei dati personali contattare immediatamente il Consorzio dei Comuni Trentini – Servizio RPD per valutare assieme:

- quanto occorso;
- gli elementi caratterizzanti il caso;
- le azioni e le misure da adottarsi.