COMUNE DI TELVE DI SOPRA

(Provincia di Trento)

Verbale di deliberazione N. 93

della Giunta comunale

OGGETTO: **Approvazione "Procedura per la gestione delle violazioni dei dati personali ('data breach') del Comune di Telve di Sopra".**

L'anno **DUEMILAVENTICINQUE** addì **cinque** del mese di **dicembre**, alle ore 08.50, nella sala delle riunioni, formalmente convocato si è riunita la Giunta comunale.

Presenti i signori:

	Assenti	
	giust.	ingiust.
1. Bonella Giampaolo - Sindaco		
2. Trentin Andrea - Vicesindaco		
3. Borgogno Giulia - Assessore		
4. Trentin Sergio - Assessore	**X**	

Assiste il Segretario Generale Comite dott.ssa Maria.

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

OGGETTO: Approvazione "Procedura per la gestione delle violazioni dei dati personali ('data breach') del Comune di Telve di Sopra".

LA GIUNTA COMUNALE

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") e in data 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;

Tale Regolamento, denominato "Regolamento generale sulla protezione dei dati", in sigla GDPR, detta la disciplina in materia del trattamento dei dati personali, prevedendo tra gli elementi caratterizzanti e innovativi il "principio di responsabilizzazione" (c.d. accountability) e pone al centro del quadro normativo la figura del "Responsabile della protezione dei dati", in sigla RPD.

Alla luce di quanto sopra, con deliberazioni n. 46 di data 05.06.2018 per il 2018 e 2019, n. 18 di data 03.03.2020 per il 2020, n. 13 di data 01.03.2021 per il 2021, n.12 di data 07.03.2022 per il 2022 e 2023, n. 109 di data 28.12.2023 per il 2024 e da ultimo con la n. 92 di data 18.12.2024 per l'anno 2025, la Giunta comunale, per le ragioni ivi contenute, ha affidato al Consorzio dei Comuni Trentini, il servizio di consulenza in materia di "privacy" e la nomina come Responsabile della Protezione dei Dati (RPD) ai sensi del regolamento europeo 2016/679;

In riferimento alla designazione obbligatoria della figura del Responsabile della protezione dei Dati RPD prevista dall'art. 37 del suddetto regolamento, con nota del Consorzio dei comuni trentini del 15.01.2024 prot. com.le n. 222 di data 22.01.2024 è pervenuta la comunicazione della modifica del referente presso l'autorità garante per la protezione dei dati personali, individuata nella persona fisica della dott.ssa Laura Marinelli che è referente e punto di contatto con il Garante privacy sulla base dell'art. 39, paragrafo 1, lettera e) del Regolamento (UE) 2016/679;

Dato atto che in data 07.02.2024 è stata registrata la comunicazione di variazione del referente indicato in precedenza, al garante per la protezione dei dati personali;

In relazione a quanto sopra, si evidenzia che, ai sensi degli art. 33 e 34 del Regolamento (UE) 2016/679, nei casi di violazione dei dati personali, il Comune è tenuto a comunicarlo al Garante per la protezione dei dati personali e, se si rappresenta un rischio elevato per i diritti e le libertà delle persone fisiche, anche all'interessato.

Ricordato che per «violazione dei dati personali» si intende 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 (art. 4, punto 12 del Regolamento; art. 2, comma 1, lett. m, del d.lgs. n. 51/2018) e che in caso di violazione dei dati personali, il titolare del trattamento è tenuto a notificare tale evento al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (artt. 33 e 55 del Regolamento 679/2016, art. 2-bis del D. Lgs. 196/2003);

Preso atto che il Garante Privacy ha ritenuto necessario, per accrescere l'efficacia e l'efficienza dell'azione amministrativa e, nel contempo, semplificare l'adempimento degli obblighi da parte dei

titolari del trattamento, adottare un'apposita procedura telematica per la notifica della violazione dei dati personali nonché individuare le informazioni da fornire al Garante ai sensi dell'art. 33 del Regolamento 679/2016 e art. 26 del D.lgs. 18 maggio 2018, n. 51;

Dato atto che con Provvedimento del Garante Privacy del 27 maggio 2021, a decorrere dal 01 luglio 2021 la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica disponibile nel portale dei servizi online dell'Autorità Garante della Privacy, per il corretto adempimento dell'obbligo di cui all'art. 33 e 55 del Regolamento 679/2016 e dell'art. 2-bis del Codice;

Tutto ciò premesso e considerato l'Amministrazione comunale intende approvare la "Procedura per la gestione della violazione dei dati personali (DATA BREACH) del Comune di Telve" rinnovata e attualizzata, che costituisce allegato parte integrante della presente (allegato A);

Visto il D.lgs. 30.06.2003, n. 196 – Codice della Privacy;

Visto il Regolamento (UE) 2016/679;

Visto il D.Lgs. 10.08.2018 n. 101;

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 generale in ordine alla regolarità tecnico-amministrativa espresso;

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;

Visto il Codice degli Enti Locali della Regione Autonoma Trentino Alto Adige approvato con L.R. 3 maggio 2018, n. 2 e ss.mm;

Visto lo Statuto comunale.

Accertata la propria competenza

Ad unanimità di voti espressi per alzata di mano

D E L I B E R A

1. Di adottare la "Procedura per la gestione delle violazioni dei dati personali ('data breach') del Comune di Telve di Sopra" rinnovata e attualizzata, di cui agli artt. 33 e 34 del Regolamento (UE) 2016/679, che costituisce allegato parte integrante e sostanziale alla presente deliberazione (allegato A);

2. di demandare a separato provvedimento del Titolare del Trattamento, l'effettuazione della designazione del Referente della gestione delle violazioni dei dati personali, c.d. "referente data breach" individuata nella persona del Segretario comunale;

3. di incaricare il Segretario comunale, nella sua qualità di referente privacy dell'Ente, di garantire una adeguata informazione al personale dipendente e agli altri soggetti interessati (Amministratori, Collaboratori, dipendenti etc.) in ordine alla procedura di cui al primo punto e

all’osservanza della presente procedura secondo il modello di comunicazione che costituisce allegato parte integrante e sostanziale alla presente (allegato B) e che contestualmente si approva;

4. di dare atto che la presente diverrà esecutiva decorsi dieci giorni dalla pubblicazione, ai sensi dell’articolo 183 comma 3 del Codice degli Enti locali della Regione Autonoma Trentino Alto-Adige, approvato con Legge Regionale 03.05.2018, n. 2;

5. di trasmettere la presente deliberazione ai capigruppo consiliari ai sensi e per gli effetti del disposto dell’art. 183, comma 3 del Codice Enti Locali approvato con L.R. 03.05.2018 n. 2;

6. di dare evidenza che, 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 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

Letto, approvato e sottoscritto.

IL SINDACO	IL SEGRETARIO GENERALE
Bonella Giampaolo	Comite dott.ssa Maria

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).

Allegato A

PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI
(DATA BREACH)
DEL COMUNE DI TELVE DI SOPRA

Documento approvato con Delibera di data		
Revisione	Data	Motivo
	/12/2025	Aggiornamento procedura

INDICE

1 SCOPO 3
2 AGGIORNAMENTO 3
3 DEFINIZIONI 3
4 ORGANIZZAZIONE DELLE ATTIVITÀ DI GESTIONE DELL'EVENTO VIOLAZIONE DEI DATI PERSONALI 3
5 GESTIONE DELLE ATTIVITÀ CONSEGUENTI AD UNA POSSIBILE VIOLAZIONE DI DATI PERSONALI 4
6 NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ GARANTE 4
7 COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI AGLI INTERESSATI 4
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 del Comune di Telve di Sopra 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 alla Giunta comunale 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 coincide con il Referente privacy dell'Ente, entrambi individuati nel Segretario comunale pro tempore.
- comunicare i nominativi del Referente privacy e del Referente data breach a tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali del Comune di Telve di Sopra;
- 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 del Comune di Telve di Sopra;
- 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 il Comune di Telve di Sopra, viene a conoscenza di una possibile violazione dei dati personali, deve immediatamente segnalare l'evento al Segretario comunale in qualità di Referente Privacy e Referente data breach del Comune di Telve di Sopra 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 Segretario comunale quale 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 individuato nel Consorzio dei Comuni trentini 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;
- 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 e allegato alla presente procedura.

Il Consorzio dei Comuni Trentini quale 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 dal Segretario comunale nelle vesti di Referente della gestione delle violazioni dei dati personali e Referente Privacy del Comune di Telve di Sopra, 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 Segretario comunale quale 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.

POTENZIALE VIOLAZIONE DI DATI PERSONALI

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 _____

Allegato B

Alla c.a. Dipendenti e Amministratori
Del Comune di Telve di Sopra

Oggetto: procedura di violazione dei dati personali (c.d. DATA BREACH)

La presente per comunicare l'aggiornamento della procedura di data breach, approvata con deliberazione della Giunta …. n… d.d…. che disciplina l'iter da seguire in caso di violazione di dati personali.

I riferimenti normativi si rinvengono negli articoli 33 e 34 del Regolamento UE 679/2016 e nelle Linee guida del Gruppo "Articolo 29" in materia di notifica delle violazioni dei dati personali (Linee guida 9/2022 in materia di notifica delle violazioni di dati personali; Linee guida EDPB 01/2021 sugli esempi riguardanti la notifica di violazione dei dati).
Per data breach si intende una violazione di sicurezza che comporta una violazione dei dati personali in termini di:

- 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, ossia indebita o accidentale alterazione dei dati personali.

1. Gestione interna del data breach seguendo l'apposita procedura adottata dall'Ente

In caso di supposta violazione di dati personali deve essere avvisato tempestivamente il Segretario comunale quale Referente Data breach e il Referente Privacy del Comune di Telve di Sopra affinchè:

- Vengano adottate le Misure di sicurezza informatiche e/o organizzative per porre rimedio o attenuare i possibili effetti negativi della violazione dei dati personali e, contestualmente, venga informato immediatamente il Consorzio dei Comuni Trentini quale Responsabile della Protezione dei Dati per una valutazione condivisa;
- Venga condotta e documentata 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".

2. 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 l'Ente ne è venuto a conoscenza, 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 dovrà essere documentato il motivo del ritardo. La notifica deve contenere una serie di elementi come indicati nella norma, e 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.

La notifica deve avvenire telematicamente attraverso il portale messo a disposizione dall'Autorità Garante al seguente link: https://servizi.gpdp.it/databreach/s/

3. 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 deve comunicare la violazione all'interessato senza ingiustificato ritardo. In presenza di alcune condizioni non è necessaria la comunicazione all'interessato.

4. Registro delle violazioni

Deve essere formato un Registro delle violazioni i dati personali e, nel caso si verifichi un evento che comporti, o possa comportare, una violazione dei dati personali, oltre a quanto sopra indicato, andrà compilato il Registro con le informazioni necessarie a gestire l'evento, tra cui quanto occorso; gli elementi caratterizzanti il caso; le azioni e le misure migliorative da adottarsi.

5. Esempi di violazioni

	Violazione
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. (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).
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).
4	Il locale archivio dell'ente subisce una effrazione e il furto di alcuni faldoni contenenti dati personali.
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.
6	A seguito di un attacco informatico ad un servizio online dell'ente vengono prelevati e diffusi dati personali degli utenti.

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).
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.
9	Un cittadino segnala di aver ricevuto per sbaglio documentazione contenente dati personali relativi ad altri soggetti.
10	Una e-mail contenente dati personali viene inviata per sbaglio ad un elevato numero di destinatari.

6. Formazione

Al fine di riconoscere una violazione di dati personali e tutti gli adempimenti necessari per evitarla, è necessario che tutti i dipendenti e gli amministratori siano costantemente informati e formati in materia di protezione dati personali.