



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

Documento approvato con Delibera della Giunta comunale di data 11 dicembre 2018 n. 90

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.....	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 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.

(Opzione facoltativa) In ragione della struttura organizzativa dell'Ente, il Titolare designa un gruppo di lavoro, denominato Gruppo di gestione delle violazioni dei dati personali, che supporta il suddetto Referente e di cui lo stesso funge da coordinatore.

Il Gruppo è formato da personale avente professionalità rilevanti in materia di trattamento di dati personali per i diversi profili di interesse (competenza informatica, legale, contrattualistica, ecc.);

- 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 serviziordpd@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.



COMUNE DI VARENA

Via Mercato 16 – 38030 VARENA (TN)

SERVIZIO RESPONSABILE DELLA PROTEZIONE DEI DATI

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



VIOLAZIONE DI DATI PERSONALI
MODELLO DI COMUNICAZIONE AL GARANTE

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

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 _____

[illegible]

Pagina 1 di 4