



COMUNE DI SPORMINORE

PROVINCIA DI TRENTO

Piazza Anaunia n. 4

Tel. 0461/641118 - Fax 0461/641110
P. IVA 00443750229 - C.F. 80009570229
e-mail: info@comune.sporminore.tn.it
pec: comune@pec.comune.sporminore.tn.it

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

Documento approvato con Delibera n. 20 di data 19/02/2020

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 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.

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

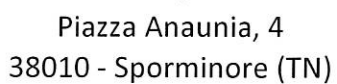
modalità di comunicazione di tale violazione agli interessati, come previsto dall'art. 34 del Regolamento europeo n. 679 del 2016.

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.

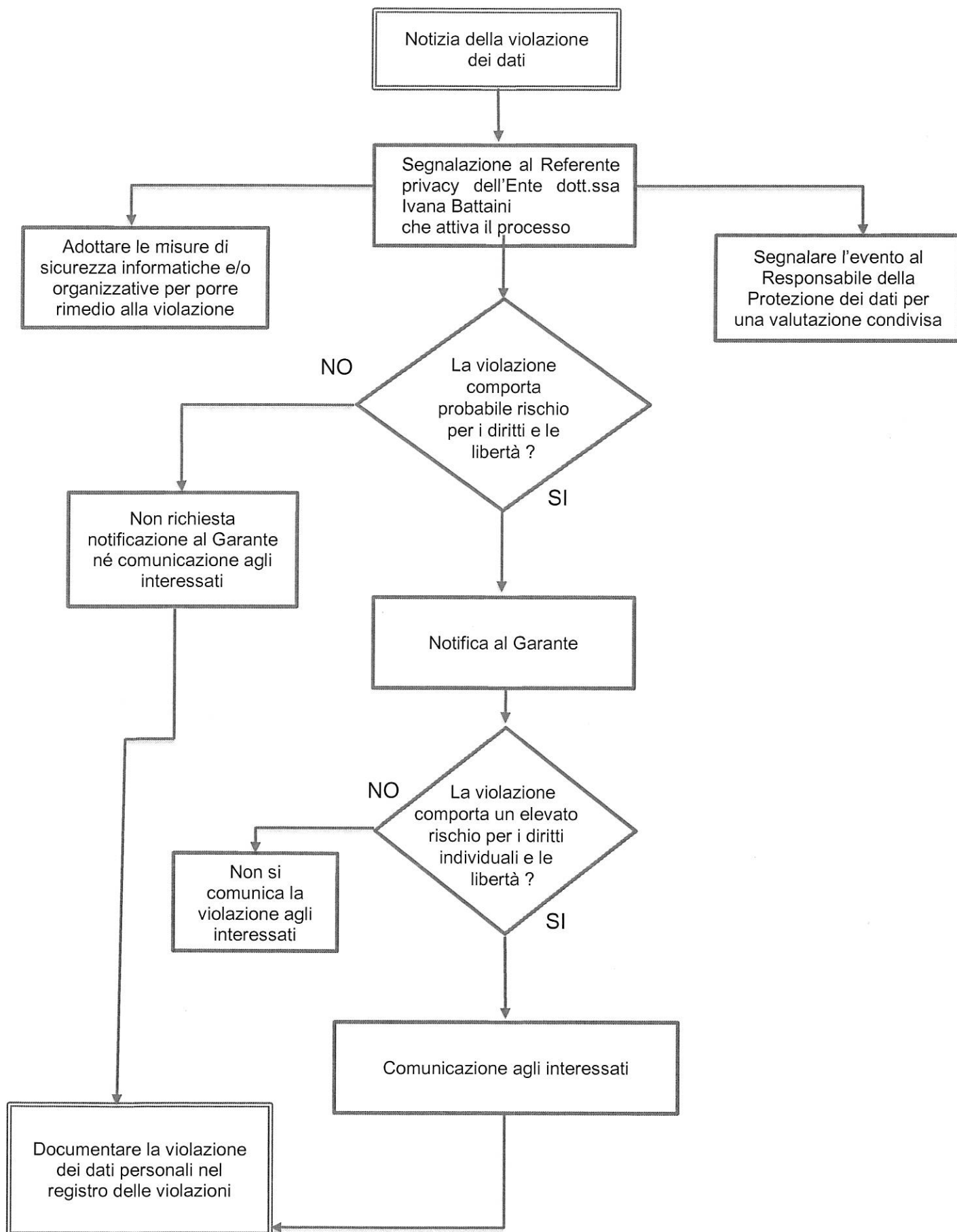
Per la redazione del registro è possibile ricorrere al sistema di fascicolazione se disponibile nel programma di gestione documentale dell'Ente o ad un file excel.



Allegato n. 1

[illegible]

Il flusso degli adempimenti in caso di violazione dei dati





COMUNE DI SPORMINORE

PROVINCIA DI TRENTO

Piazza Anaunia n. 4

Tel. 0461/641118 - Fax 0461/641110
P. IVA 00443750229 - C.F. 80009570229
e-mail: info@comune.sporminore.tn.it
pec: comune@pec.comune.sporminore.tn.it

Allegato n. 3

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

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 _____

**COMUNE DI SPORMINORE**

PROVINCIA DI TRENTO

Piazza Anaunia n. 4

Tel. 0461/641118 - Fax 0461/641110
P. IVA 00443750229 - C.F. 80009570229
e-mail: info@comune.sporminore.tn.it
pec: comune@pec.comune.sporminore.tn.it

Allegato n. 4

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
<p>La banca dati è denominata "Banche dati dei clienti della Banca di Sicilia" e contiene i dati personali dei clienti della Banca di Sicilia, ivi compresi i dati personali dei clienti della Banca di Sicilia che sono stati oggetto di data breach.</p> <p>La violazione dei dati personali ivi trattati consiste nel fatto che i dati personali dei clienti della Banca di Sicilia sono stati oggetto di data breach.</p>



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?