PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI DEL COMUNE DI CANAZEI "DATA BREACH"

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.

Organizzazione delle attività di gestione dell'evento violazione dei dati personali

Il Titolare ha designato un Referente della gestione delle violazioni dei dati personali (di seguito Referente "data breach"), nella figura del Segretario comunale, oltre che, con decreto sindacale n. 7 d.d. 12.09.2024 ha costituito un gruppo di lavoro privacy nominando il Segretario comunale e la dipendente matricola 202.

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" 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 al 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 del 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 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 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.

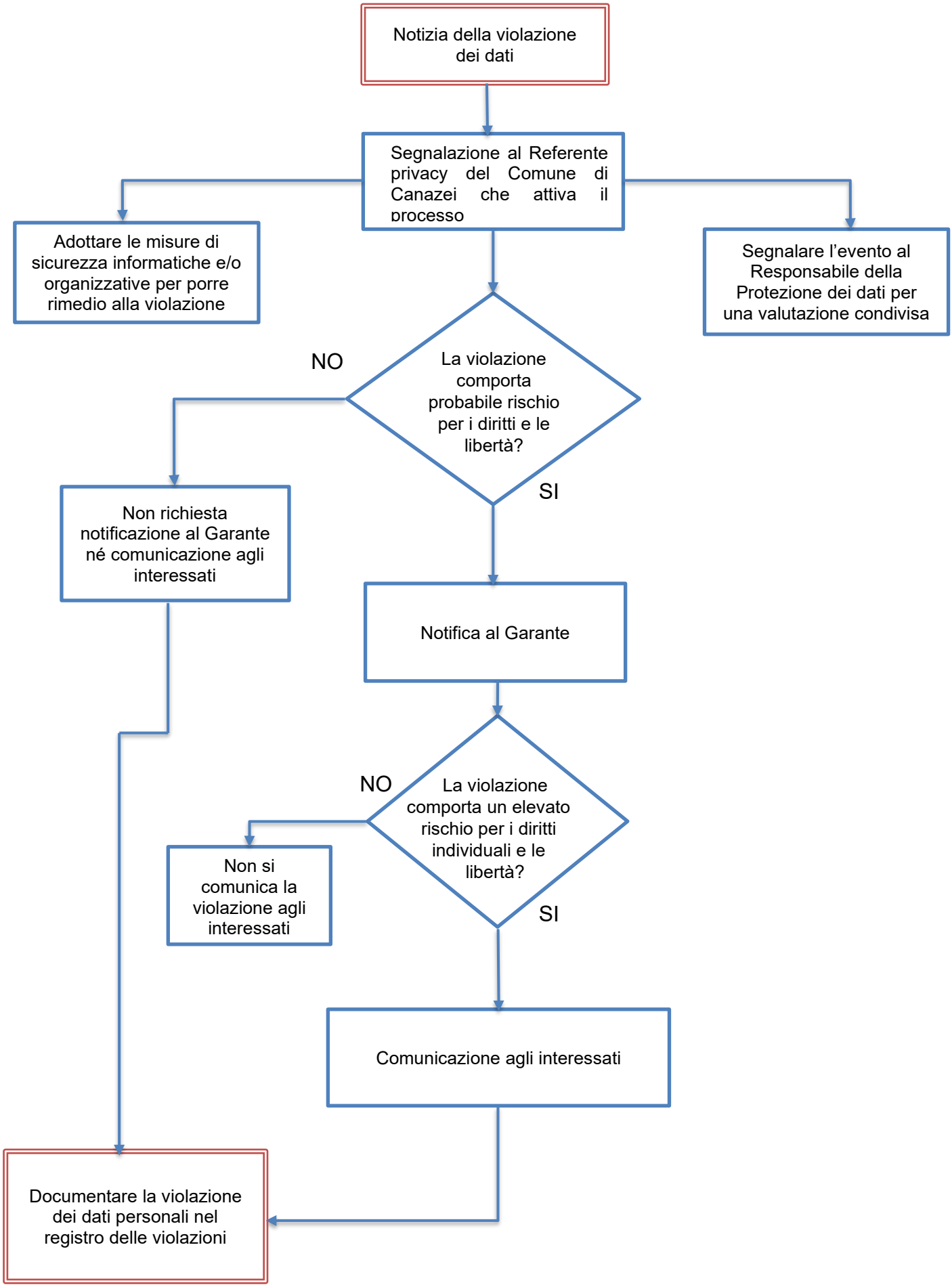
Tale documento è tenuto e implementato dal Referente "data breach", e consente all'autorità di controllo di verificare il rispetto dall'art. 33 del Regolamento europeo n. 679 del 2016.

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.

Allegati:

1. flusso degli adempimenti in caso di violazione dei dati personali;
2. modello di potenziale violazione dei dati personali al Responsabile Protezione Dati – RPD;
3. modello comunicazione violazione all'Autorità Garante.

Il flusso degli adempimenti in caso di violazione dei dati



POTENZIALE VIOLAZIONE DEI DATI PERSONALI
MODELLO DI COMUNICAZIONE
AL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

ENTE: COMUNE DI CANAZEI

REFERENTE PRIVACY E DATA BREACH DELL'ENTE: SEGRETARIO COMUNALE

TELEFONO: 0462605626 MAIL: segretario@comune.canazei.tn.it PEC: protocollo: protocollo.comunecanazei@pec.it

NOME E COGNOME DEL SEGNALANTE:

_____

INDICARE LA VIOLAZIONE DEI DATI PERSONALI:

_____

_____

_____

_____

_____

_____

DENOMINAZIONE DELLA BANCA DATI OGGETTO DI DATA BREACH E DESCRIZIONE DEI DATI PERSONALI IVI TRATTATI:

_____

_____

_____

_____

_____

_____

INDICARE LE MODALITÀ DI VIOLAZIONE DEI DATI PERSONALI (SPECIFICANDO SE VI È STATO LO SMARRIMENTO DI DISPOSITIVI PORTATILI FUORI DALL'ENTE) E LA DATA IN CUI LA VIOLAZIONE È AVVENUTA:

_____

_____

_____

_____

_____

_____

INDICARE L'ESPOSIZIONE AL RISCHIO (BARRARE LE IPOTESI RELATIVE ALLA VIOLAZIONE):

- LETTURA DEI DATI (SENZA COPIATURA)
- COPIA DEI DATI (I DATI SONO IN POSSESSO DEL COMUNE MA SONO STATI COPIATI)
- ALTERAZIONE DEI DATI PRESENTI SU SISTEMI DEL COMUNE
- CANCELLAZIONE DEI DATI DA SISTEMI DEL COMUNE
- FURTO (I DATI NON SONO PRESENTI SU SISTEMI DEL COMUNE E NON SONO IN POSSESSO DELL'AUTORE DELLA VIOLAZIONE)
- ALTRA IPOTESI
  _____

DISPOSITIVO OGGETTO DI VIOLAZIONE (BARRARE LE IPOTESI INTERESSATE):

- COMPUTER
- RETE
- DISPOSITIVO MOBILE
- FILE
- BACK UP DI FILE
- DOCUMENTO CARTACEO
- SOFTWARE
- SERVIZIO INFORMATICO
- ALTRO

_____

INDICARE SE LA VIOLAZIONE HA INTERESSATO UNA PERSONA O PIU' DI UNA PERSONA:

_____

_____

INDICARE CHE TIPO DI DATI SONO STATI VIOLATI (BARRARE I DATI INTERESSATI DALLA VIOLAZIONE):

- DATI PERSONALI (COMPRESO IL CODICE FISCALE)
- DATI DI ACCESSO A SISTEMI O A SITI (PASSWORD - USERNAME - ECC.)
- DATI RELATIVI A MINORI

- DATI IDONEI A RILEVARE LE ORIGINI ETNICHE, RAZIALI, DI CONVINZIONE RELIGIOSA, FILOSOFICA O ALTRO, LE OPINIONI POLITICHE, L'ADESIONE A PARTITI, ASSOCIAZIONI

- DATI GIUDIZIARI

- COPIA DI IMMAGINE SU SUPPORTO INFORMATICO DI DOCUMENTO ANALOGICO

- ALTRO
  _____

INDICARE I FORNITORI ESTERNI O ALTRI SOGGETTI ESTERNI COINVOLTI SE ESISTENTI:

_____

_____

_____

_____

_____

INDICARE LE MISURE TECNICHE APPLICATE DALL'ENTE ALLA VIOLAZIONE SE GIA' CONOSCIUTE:

_____

_____

_____

_____

_____

DATA _____

IL SEGNALANTE

_____

POTENZIALE VIOLAZIONE DEI DATI PERSONALI
MODELLO DI COMUNICAZIONE
AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

ENTE: COMUNE DI CANAZEI

INDIRIZZO: STREDA ROMA 12 CANAZEI (TN)

NOME DELLA PERSONA ADDETTA ALLA COMUNICAZIONE: SINDACO PRO TEMPORE

TELEFONO: 0462605626

PEC: protocollo.comunecanazei@pec.it

RESPONSABILE PROTEZIONE DEI DATI PERSONALI: CONSORZIO DEI COMUNI TRENTINI VIA TORRE VERDE 23 TRENTO (TN) TELEFONO: 0461987139
PEC: consorzio@pec.comunitrentini.it

INDICARE LA VIOLAZIONE DEI DATI PERSONALI CON SINTETICA DESCRIZIONE DEI SISTEMI DI ELABORAZIONE O MEMORIZZAZIONE COINVOLTI:

_____

_____

_____

_____

_____

_____

DENOMINAZIONE DELLA BANCA DATI OGGETTO DI DATA BREACH E DESCRIZIONE DEI DATI PERSONALI IVI TRATTATI:

_____

_____

_____

_____

_____

_____

INDICARE LE MODALITÀ DI VIOLAZIONE DEI DATI PERSONALI (SPECIFICANDO SE VI È STATO LO SMARRIMENTO DI DISPOSITIVI PORTATILI FUORI DALL'ENTE) E LA DATA IN CUI LA VIOLAZIONE È AVVENUTA:

_____

_____

_____

_____

_____

_____

INDICARE L'ESPOSIZIONE AL RISCHIO (BARRARE LE IPOTESI RELATIVE ALLA VIOLAZIONE):

- LETTURA DEI DATI (SENZA COPIATURA)
- COPIA DEI DATI (I DATI SONO IN POSSESSO DEL COMUNE MA SONO STATI COPIATI)
- ALTERAZIONE DEI DATI PRESENTI SU SISTEMI DEL COMUNE
- CANCELLAZIONE DEI DATI DA SISTEMI DEL COMUNE
- FURTO (I DATI NON SONO PRESENTI SU SISTEMI DEL COMUNE E NON SONO IN POSSESSO DELL'AUTORE DELLA VIOLAZIONE)

- ALTRA IPOTESI

  _____

DISPOSITIVO OGGETTO DI VIOLAZIONE (BARRARE LE IPOTESI INTERESSATE):

- COMPUTER
- RETE
- DISPOSITIVO MOBILE
- FILE
- BACK UP DI FILE
- DOCUMENTO CARTACEO
- SOFTWARE
- SERVIZIO INFORMATICO
- ALTRO

  _____

INDICARE SE LA VIOLAZIONE HA INTERESSATO UNA PERSONA O PIU' DI UNA PERSONA:

_____

_____

INDICARE CHE TIPO DI DATI SONO STATI VIOLATI (BARRARE I DATI INTERESSATI DALLA VIOLAZIONE):

- DATI PERSONALI (COMPRESO IL CODICE FISCALE)
- DATI DI ACCESSO A SISTEMI O A SITI (PASSWORD - USERNAME - ECC.)

- DATI RELATIVI A MINORI
- DATI IDONEI A RILEVARE LE ORIGINI ETNICHE, RAZIALI, DI CONVINZIONE RELIGIOSA, FILOSOFICA O ALTRO, LE OPINIONI POLITICHE, L'ADESIONE A PARTITI, ASSOCIAZIONI
- DATI GIUDIZIARI
- COPIA DI IMMAGINE SU SUPPORTO INFORMATICO DI DOCUMENTO ANALOGICO
- ALTRO
  _____

CLASSIFICARE LA VIOLAZIONE IN BASE AL RISCHIO CHE COMPORTA (1 BASSO / 2 MEDIO / 3 ALTO / 4 ALTISSIMO)

_____

INDICARE I FORNITORI ESTERNI O ALTRI SOGGETTI ESTERNI COINVOLTI SE ESISTENTI:

_____

_____

_____

_____

_____

_____

INDICARE LE MISURE TECNICHE APPLICATE DALL'ENTE ALLA VIOLAZIONE ATTE A CONTENERE LA MEDESIMA E LA VIOLAZIONE DEI DATI FUTURI:

_____

_____

_____

_____

_____

_____

INDICARE SE LA VIOLAZIONE È STATA COMUNICATA DALL'ENTE AGLI INTERESSATI RIPORTANDO (ANCHE IN ALLEGATO) IL CONTENUTO DELLA COMUNICAZIONE:

_____

_____

_____

_____

_____

_____

DATA _____

IL SINDACO

_____