COMUNITÁ DELLA
VAL DI NON

Via Pilati, n. 17
38023 - Cles (TN)

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI ("*DATA BREACH*")

Documento approvato con deliberazione del Comitato esecutivo n. 112 di data 06.11.2018		
Revisione	Data	Motivo

INDICE

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 degli obblighi relativi alla notifica all'Autorità Garante per la protezione dei dati personali e alla comunicazione all'interessato ed in ossequio alle previsioni di cui agli artt. 33 e 34 del Regolamento (UE) 2016/679.

Tutti i soggetti (Amministratori, Dipendenti, Collaboratori, etc.) 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'art. 4 del Regolamento (UE) 2016/679:

«**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'art. 51 del Regolamento(UE) 2016/679.

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

Il Titolare del trattamento deve:

- designare un Referente della gestione delle violazioni dei dati personali, di seguito semplicemente denominato "Referente data breach", figura che può coincidere con il Referente privacy dell'ente.
- comunicare il nome del designato a tutti i soggetti (Amministratori, Dipendenti, Collaboratori, etc.) 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 dei 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, etc.) attraverso la compilazione del "*Modello di potenziale violazione dei dati personali al Responsabile Protezione Dati*";
- riferire i risultati dell'indagine inviando il Modello di cui al punto precedente all'indirizzo serviziorpd@comunitrentini.it del Responsabile della Protezione dei Dati, al Referente privacy dell'ente e al Titolare del trattamento.

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, circa il fatto se quest'ultimo configuri o meno una violazione dei dati personali e se lo stesso possa comportare o meno un probabile rischio per i diritti e le libertà delle persone fisiche.
Lo invia quindi al Referente data breach, al Referente privacy dell'ente e al Titolare del trattamento.

6 Notifica della violazione dei dati personali all'Autorità Garante

Il Titolare del trattamento – tenuto conto del parere formulato dal Responsabile della Protezione dei Dati e dalle valutazioni fatte congiuntamente dal Referente data breach 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 (UE) 2016/679 .

7 Comunicazione della violazione dei dati personali agli interessati

Il Titolare del trattamento, 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 precedente punto 6, decide le modalità di comunicazione di tale violazione agli interessati, come previsto dall'art. 34 del Regolamento (UE) 2016/679.

8 Compilazione del Registro delle violazioni dei dati personali

Il Titolare del trattamento, 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 di quanto disposto dall'art. 33 del Regolamento (UE) 2016/679.
Per la redazione del Registro delle violazioni dei dati personali è possibile ricorrere al sistema di fascicolazione se disponibile nel programma di gestione documentale dell'ente o ad un file excel.

Allegati alla presente procedura:

- Registro delle violazioni dei dati personali;
- Flusso degli adempimenti in caso di violazione dei dati personali;
- Modello di potenziale violazione dei dati personali al Responsabile Protezione Dati;
- Modello comunicazione violazione all'Autorità Garante.

COMUNITÁ DELLA
VAL DI NON

Via Pilati, n. 17
38023 - Cles (TN)

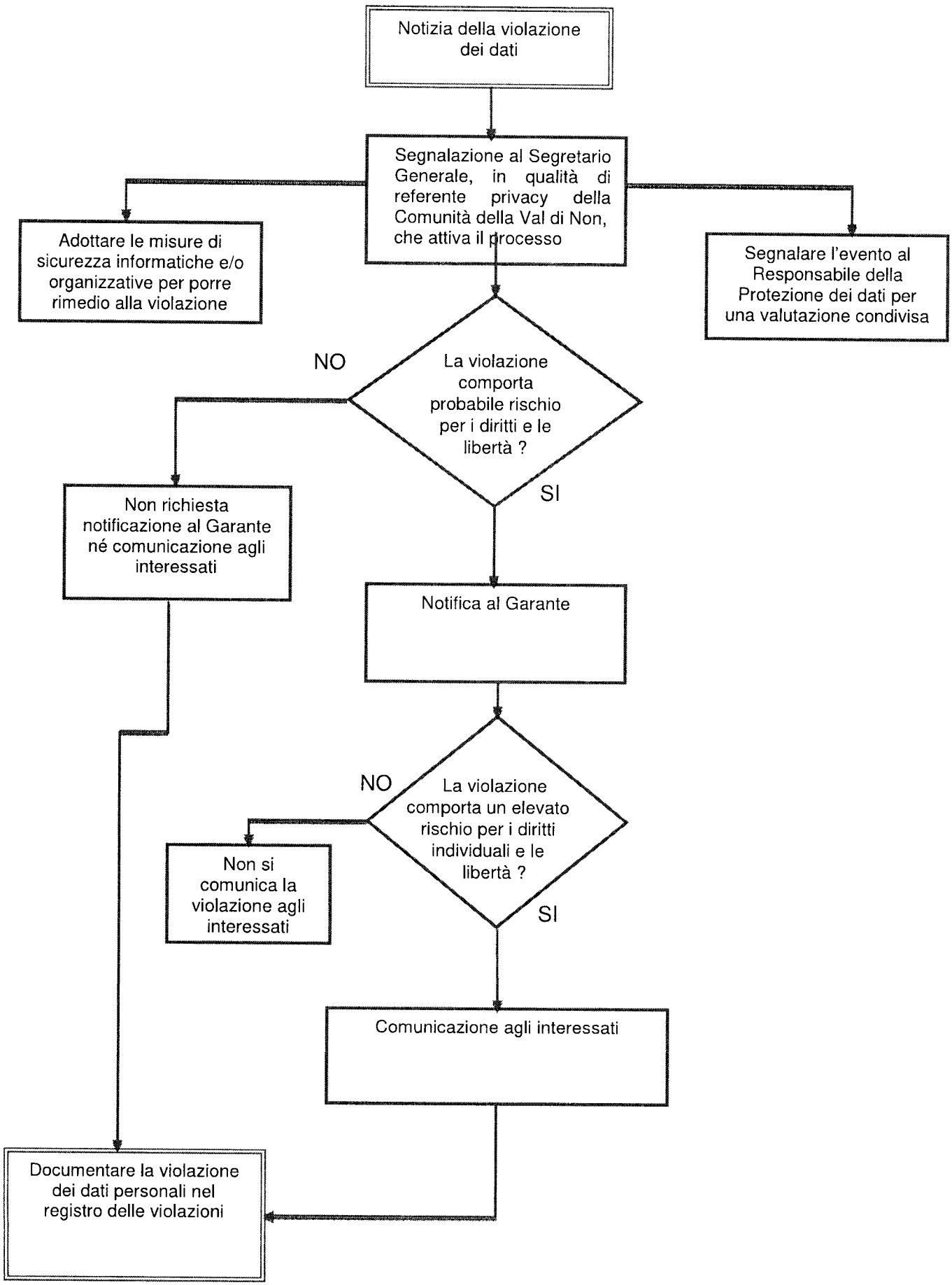
allegato n. 1

PROCEDURA DATA BREACH
REGISTRO DELLE VIOLAZIONI

n. pr.	data evento	descrizione evento	possibili conseguenze della violazione	misure adottate	comunicazione al garante	comunicazione agli interessati

allegato n. 2

PROCEDURA DATA BREACH
Il flusso degli adempimenti in caso di violazione dei dati



COMUNITÁ DELLA
VAL DI NON

Via Pilati, n. 17
38023 - Cles (TN)

Allegato 3

POTENZIALE VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL RESPONSABILE DELLA PROTEZIONE DEI DATI

Ente _____

Referente data breach _____

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 _____ 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 _____

COMUNITÁ DELLA
VAL DI NON

Via Pilati, n. 17
38023 - Cles (TN)

Allegato 4

VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dall'art. 33 del Regolamento (UE) 2016/679, il Titolare del trattamento 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.

Ente titolare del trattamento

Denominazione o ragione sociale: Comunità della Val di Non
Provincia di Trento – Comune: Cles

Cap: 38054 Indirizzo: via C.A. Pilati n. 17 - Cles

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

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 _____ 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?