

COMUNE DI CAMPITELLO DI FASSA
PROVINCIA DI TRENTO



COMUN DE CIAMPEDEL
PROVINCIA DE TRENT

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE
VERBAL DE DELIBERAZION DE LA JONTA DE COMUN

N. **006**

OGGETTO: APPROVAZIONE SCHEMA DI PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH).

ARGOMENT: [...].

L'anno DUEMILAVENTI addì DIECI del mese di FEBBRAIO alle ore 11.15 nella sala delle riunioni, a seguito di regolari avvisi, recapitati a termine di legge, si è convocata la Giunta comunale.

L'an DOIMILEVINT ai DIESE de FIRE' da les 11.15 te sala de la adunançes, dò aer manà fora l'avis aldò de la lege, se à binà la Jonta de Comun.

Sono presenti i signori/*Tol pèrt i Segnores:*

BERNARD IVO	<i><u>Sindaco</u></i>
SOMMAVILLA STEFANO	<i><u>Vicesindaco</u></i>
CAPOVILLA MANUEL	<i><u>Assessore</u></i>

ASSESSORE ROBERTA CREBELLI ASSENTE GIUSTIFICATA

Assiste il Segretario comunale Sensato dr. Graziano

Tol Pèrt e verbalisea l Segretèr de Comun Sensato dr. Graziano

Il signor BERNARD IVO nella sua qualità di Sindaco da atto che sono verificate le condizioni previste dall'art. 3 del Regolamento della Giunta comunale approvato con deliberazione del Consiglio comunale n. 19 del 02.08.2019 e riconosciuto legale il numero degli intervenuti, assume la presidenza e dichiara aperta la seduta per la trattazione dell'oggetto suindicato.



PROPOSTA DI DELIBERAZIONE DELLA GIUNTA COMUNALE

APPROVAZIONE SCHEMA DI PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH).

Vista la proposta di deliberazione e la documentazione di supporto ed istruttoria, si esprime:

- in ordine alla regolarità tecnico - amministrativa (art. 185 L.R. 03.05.2018 n. 2) parere:

Favorevole

Non Necessario

NON Favorevole

Lì, 10.02.2020

Il Segretario comunale
f.to dott. Sensato Graziano

- in ordine alla regolarità contabile (art. 185 L.R. 03.05.2018 n. 2) parere:

Favorevole

Non Necessario

NON Favorevole

Lì, 10.02.2020

-
f.to -

Deliberazione della Giunta comunale n. 06 dd. 10/02/2020
Pubblicata all'albo comunale in data 25.02.2020

OGGETTO: Approvazione schema di procedura per la gestione della violazione dei dati personali (DATA BREACH).

Premesso che:

- la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale;
- l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea ("Carta") e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione Europea ("TFUE") stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;
- 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");
- il 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;
- il Regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi, effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione;
- in esecuzione del GDPR ed al fine di attuare un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, è richiesto alle aziende e alle Pubbliche Amministrazioni di approntare un piano di protezione dei dati personali che, partendo dalla mappatura e dall'analisi dei trattamenti, effettui la valutazione del rischio di violazione ed individui infine le misure volte ad eliminare o almeno ridurre il rischio stesso;
- dato atto che permane comunque la possibilità che i dati personali vengano violati da parte di soggetti terzi, e che si rende quindi necessario prevedere una procedura da attuare nel caso si verificasse l'evento in questione.

LA GIUNTA COMUNALE

Visto lo schema di procedura per la gestione della violazione dei dati personali (DATA BREACH) predisposto dal Consorzio dei Comuni, con sede a Trento in via Torre Verde n. 23, in qualità di Responsabile della Protezione dei dati del Comune di Campitello di Fassa, che 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;

Visti gli allegati allo schema di cui sopra, ed in particolare:

- Allegato A: potenziale violazione di dati personali - modello di comunicazione al responsabile della protezione dei dati;
- Allegato B: violazione di dati personali - modello di comunicazione al garante;

Ritenuto il predetto schema, con i relativi allegati, meritevole di approvazione;

Visto il Regolamento UE n. 679/2016;

Viste le indicazioni fornite dall'Autorità Garante per la Protezione dei Dati personali e dal Responsabile Protezione Dati del Comune di Campitello di Fassa;

Visto il Codice Enti Locali della Regione Autonoma Trentino Alto Adige, approvato con L.R. 03.05.2018 n. 2 e s.m.;

Visto il parere espresso ai sensi dell'art. 185 del Codice Enti Locali, approvato con L.R. 03.05.2018 n. 2, sulla presente proposta di deliberazione:

-dal Segretario Comunale in ordine alla regolarità tecnico-amministrativa espresso in data odierna;

Dato atto che il presente provvedimento non necessita del parere di regolarità contabile di cui agli artt. 185 e 187 del Codice Enti Locali, approvato con L.R. 03.05.2018 n. 2 e s.m., in quanto non comporta impegni di spesa o diminuzioni di entrate;

Accertata la propria competenza, ai sensi dell'art. 53 della L.R. 03.05.2018 n. 2 e s.m.;

Con voti unanimi espressi nelle forme di legge

DELIBERA

1. **Di approvare** lo schema di procedura per la gestione della violazione dei dati personali (DATA BREACH), così come predisposto dal Consorzio dei Comuni, con sede a Trento in via Torre Verde n. 23, in qualità di Responsabile della Protezione dei dati del Comune di Campitello di Fassa, che 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, ivi compresi i relativi allegati "A" e "B", che allegati alla presente deliberazione ne costituisce parte integrante e sostanziale.

2. **Di disporre** che tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali dell'Ente vengano informati del presente provvedimento e osservino la presente Procedura.

3. **Di dare atto** che la presente deliberazione diverrà esecutiva dopo la pubblicazione all'albo pretorio ai sensi dell'art. 183, terzo comma, del Codice Enti Locali, approvato con L.R. 03.05.2018 n. 2 e s.m..

Ai sensi dell'articolo 4 della Legge provinciale 30 novembre 1992, n. 23, avverso il presente provvedimento 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.

In materia di aggiudicazione di appalti si richiama la tutela processuale di cui al comma 5) dell'art. 120 dell'Allegato 1) al D.Lgs. 02 luglio 2010 n. 104. In particolare: - il termine per il ricorso al Tribunale Amministrativo Regionale è di 30 giorni; - non è ammesso il ricorso sub c).



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

Documento approvato con Delibera di data		
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	3
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.
- 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 serviziordp@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.



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 _____

Data lettura del presente verbale, viene approvato e sottoscritto
Dò l'aer let chest verbal vegn aproà e sotscrit

IL PRESIDENTE/L PRESIDENT
F.to Bernard Ivo

IL SEGRETARIO/L SECRÈTER
F.to Sensato Dr. Graziano

REFERATO DI PUBBLICAZIONE/ ZERTIFICAT DE PUBBLICAZION
(Art. 183 della L.R. 03.05.2018 n. 2) - (*Art. 183 L.R. 03.05.2018 n. 2*)

Certifico Io sottoscritto Segretario comunale, su conforme dichiarazione del Messo, che copia del presente verbale viene pubblicata all'albo pretorio e sul sito www.albotelematicotn.it il giorno
Gé sotscrit Secretèr de Comun zertifiche, aldò de la declarazion del Suté, che na copia de chest verbal vegn metuda fora su l'Albo de Comun e su l sito www.albotelematicotn.it ai

25.02.2020

OVE RIMARRÀ ESPOSTA PER 10 GIORNI CONSECUTIVI-OLACHE LA RESTARÀ FORA DÒ E DÒ PER 10 DIS

CERTIFICATO DI ESECUTIVITÀ / ZERTIFICAT DE METUDA EN DOURA

- Deliberazione esecutiva dopo il decimo giorno dall'inizio della pubblicazione ai sensi dell'art. 183, 3° comma, della L.R. 03.05.2018 n. 2.
Vegn declarà che chesta deliberazion la doventarà esecutiva dò da sia publicazion, aldò del terzo coma de l'art. 183 L.R. 03.05.2018 n. 2.
- Deliberazione dichiarata, per l'urgenza, immediatamente eseguibile ai sensi dell'art. 183, 4° comma, della L.R. 03.05.2018 n. 2.
Vegn declarà che chesta deliberazion la é sobito esecutiva, aldò del quarto coma de l'art. 183 L.R. 03.05.2018 n. 2.

Addì/ai ____03.2020

Il Segretario/L Secretèr de Comun
F.to Sensato Dr. Graziano

-
- (1) Copia conforme all'originale, in carta libera per uso amministrativo.
Copia valiva che l'originèl, sun papier zenzà bol per दौरa aministrativa.

Li/ai

documento sottoscritto digitalmente
Il Segretario/L Secretèr de Comun
f.to Sensato dr. Graziano