Comunità Alta Valsugana e Bersntol

Tolgamoa'schòft Hoa Valzegu' ont Bersntol

(Provincia di Trento)

DECRETO DEL PRESIDENTE N. 124

OGGETTO: **articoli 33 e 34 del Regolamento (UE) 2016/679. Aggiornamento della procedura per la gestione delle violazioni dei dati personali "data breach".**

L'anno **DUEMILAVENTISEI**, addì **VENTIDUE** del mese di **LUGLIO**, il Presidente sig. Fontanari Andrea

EMANA

il decreto in oggetto.

Assiste il Segretario Generale, dott.ssa MARIUCCIA CEMIN.

OGGETTO: articoli 33 e 34 del Regolamento (UE) 2016/679. Aggiornamento della procedura per la gestione delle violazioni dei dati personali "*data breach*".

IL PRESIDENTE

Premesso che:
- in data 25.05.2018 è entrato in vigore il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio di data 27.04.2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- in data 19.09.2018 è entrato in vigore il D.Lgs. 10.08.2018, n. 101 di armonizzazione al Regolamento (UE) 2016/679.

Evidenziato come il Regolamento (UE) 2016/679 - denominato "*Regolamento generale sulla protezione dei dati",* in sigla RGPD - detti una nuova disciplina in materia di trattamento dei dati personali, prevedendo tra gli elementi caratterizzanti e innovativi il "*principio di responsabilizzazione*" (c.d. accountability) e ponendo al centro del nuovo quadro normativo la figura del *"Responsabile della protezione dei dati"*, in sigla RPD.

Rilevato, a tal proposito, che a decorrere dall'anno 2018 sono state affidate al Consorzio dei Comuni Trentini le prestazioni connesse al ruolo di Responsabile della Protezione Dati (abbr. RPD) della Comunità Alta Valsugana e Bersntol, ai sensi dell'art. 39 del Regolamento UE 2016/679 e del servizio "*privacy*", prestazioni in ultimo affidate per l'anno 2026 con determinazione del Responsabile del Servizio Programmazione e Diritto allo studio n. 1314 di data 21.11.2025, giusta attribuzione della competenza nell'ambito del Piano Esecutivo di Gestione dell'Ente.

Accertato come tra gli adempimenti sopra indicati rientri quello previsto dagli artt. 33 e 34 del Regolamento (UE) 2016/679, e segnatamente quello relativo all'adozione di una specifica procedura disciplinante la gestione delle violazioni dei dati personali ("*data breach*").

Richiamata la deliberazione del Comitato Esecutivo n. 29 di data 11.03.2019, ad oggetto "*Artt. 33 e 34 del Regolamento (UE) 2016/679. Adozione della procedura per la gestione delle violazioni dei dati personali ("data breach")*", con al quale è stata adottata la procedura disciplinante la gestione delle violazioni dei dati personali ("*data breach*") di cui agli artt. 33 e 34 del Regolamento (UE) 2016/679, comprensiva dei seguenti allegati:
- 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.

Vista dunque la procedura disciplinante la gestione delle violazioni dei dati personali ("*data breach*") come approvata in sede di Comitato Esecutivo in data 11.03.2019.

Vista la nota del Servizio RPD del Consorzio dei Comuni Trentini prot. arr. n. 25837 di data 24.12.2025 di trasmissione del Verbale Audit 2025 e specificatamente la parte attinente alla procedura disciplinante la gestione delle violazioni dei dati personali ("*data breach*"), che riepiloga quanto emerso a tale riguardo in sede di Audit 2025 di data 10.11.2025, ovvero la necessità di aggiornare la procedura indicando l'avvenuta nomina del Referente data breach (art. 4) e nell'aggiornamento della procedura di notifica delle violazioni all'Autorità Garante, che avverrà non più in avvalendosi del "Modello comunicazione violazione all'Autorità Garante", ma tramite procedura telematica (art. 6).

Dato atto che con atto di nomina di data 13.03.2019 il Presidente e legale rappresentante della Comunità nella sua qualità di Titolare del Trattamento Dati dell'Ente ha nominato l'Amministratore di Sistema ed il Referente della gestione delle violazioni dei dati personali (Referente "*data breach*") individuato nella figura del tecnico informatico dell'Ente.

Esaminata la proposta di aggiornamento di cui trattasi e ritenuta la stessa meritevole di approvazione in quanto dovuto aggiornamento della procedura *de qua*, rispondente alle finalità ed ai contenuti previsti dagli artt. 33 e 34 del Regolamento (UE) 2016/679 e pertanto di approvare la nuova Procedura per la gestione delle violazioni dei dati personali ("*data breach*") nella versione revisionata, come da allegato al presente atto quale parte integrante e sostanziale, comprensiva dei seguenti allegati:
- registro delle violazioni dei dati personali;
- modello di comunicazione al Responsabile Protezione Dati di potenziale violazione dei dati personali.

Visti il Piano Integrato di Attività e Organizzazione (PIAO) 2026-2028, approvato con decreto del Presidente n. 62 di data 30.03.2026, e il Codice di comportamento dei dipendenti della Comunità, approvato con deliberazione della Giunta n. 191 di data 30.12.2014.

Vista la legge provinciale n. 3 del 2006 "Norme in materia di governo dell'autonomia del Trentino" e successive modificazioni ed integrazioni ed in particolare l'art. 14, comma 7, il quale stabilisce che, per quanto non previsto dalla Legge, si applicano alla Comunità stessa, le Leggi Regionali in materia di Ordinamento dei Comuni.

Visto il Codice degli Enti locali della Regione Autonoma Trentino - Alto Adige approvato con Legge Regionale 3 maggio 2018, n. 2 e s.m.

Visto lo Statuto della Comunità Alta Valsugana e Bersntol ed in particolare l'art. 77 in base al quale gli atti regolamentari e di organizzazione del Comprensorio Alta Valsugana si applicano, in quanto compatibili, fino all'entrata in vigore della corrispondente disciplina adottata dalla Comunità.

Visto il Regolamento di attuazione dell'ordinamento finanziario e contabile degli enti locali, approvato con D.P.G.R. 27 ottobre 1999, n. 8/L.

Vista la Legge provinciale 9 dicembre 2015, n. 18 e il Decreto Legislativo 23 giugno 2011, n. 118.

Visto il Regolamento di Contabilità approvato dal Consiglio con deliberazione n. 40 di data 16 dicembre 2019 e ss.mm. e integrazioni.

Visto il Documento Unico di Programmazione 2026-2028 approvato con deliberazione del Consiglio dei Sindaci n. 46 di data 16 dicembre 2025 e il Bilancio di Previsione 2026-2028 approvato con deliberazione del Consiglio dei Sindaci n. 47 di data 16 dicembre 2025, esecutivo ai sensi di legge.

Visto il parere favorevole di regolarità tecnica espresso sul presente provvedimento dal Segretario generale ai sensi dell'articolo 185 del Codice degli Enti locali della Regione autonoma Trentino-Alto Adige, approvato con L.R. 3 maggio 2018, n. 2 e dato atto che non è necessario acquisire il parere di regolarità contabile e l'attestazione della copertura finanziaria, ai sensi dell'articolo 191 del D.Lgs. 18 agosto 2000, n. 267, in quanto il presente decreto non comporta aspetti di natura finanziaria.

Ritenuto di dichiarare il presente provvedimento immediatamente eseguibile ai sensi dell'articolo 183, comma 4, della legge regionale 3 maggio 2018, n. 2 "Codice degli Enti locali della Regione autonoma Trentino-Alto Adige", al fine di poter predisporre fin da subito tutti gli atti necessari successivi al presente provvedimento.

Vista la deliberazione del Consiglio dei Sindaci n. 13 di data 10.06.2025 con la quale ai sensi dell'art. 17 della legge provinciale 16.06.2006, n. 3 e ss.mm., è stato preso atto dell'elezione del Presidente della Comunità Alta Valsugana e Bersntol e della relativa nomina.

Accertata la propria competenza all'adozione del presente provvedimento, in conformità a quanto disposto dalla L.P. 16.06.2006, n. 3 e ss.mm., dallo Statuto della Comunità, dal Regolamento di Organizzazione degli Uffici e dei Servizi, approvato con deliberazione del Consiglio dei Sindaci n. 37 di data 12 novembre 2024 e ss. mm. e ii., e dal Piano Esecutivo di Gestione 2026-2028 approvato con decreto del Presidente n. 1 di data 16 gennaio 2026.

Tutto ciò premesso,

DECRETA

1. di approvare, per le motivazioni esposte in premessa, l'aggiornamento della procedura adottata con deliberazione del Comitato Esecutivo n. 29 di data 11.03.2019 disciplinante la gestione delle violazioni dei dati personali ("*data breach*") di cui agli artt. 33 e 34 del Regolamento (UE) 2016/679, nel testo allegato al presente per formarne parte integrante e sostanziale;

2. di dare atto che il nuovo testo di procedura di cui al precedente punto 1. risulta comprensivo dei seguenti allegati:
   - registro delle violazioni dei dati personali;
   - modello di comunicazione al Responsabile Protezione Dati di potenziale violazione dei dati personali;

3. di demandare alla Responsabile del Servizio Programmazione e Diritto allo studio, nella sua qualità di Referente privacy dell'Ente, tutti gli adempimenti atti a garantire una adeguata informazione al personale dipendente in ordine alla procedura di cui al presente atto;

4. di dichiarare il presente provvedimento immediatamente eseguibile ai sensi dell'articolo 183, comma 4 del Codice degli Enti locali della Regione Autonoma Trentino - Alto Adige, approvato con Legge regionale 3 maggio 2018, n. 2, per le motivazioni espresse in premessa;

5. di dare evidenza, ai sensi dell'art. 4 della Legge provinciale 30 novembre 1992, n. 23, che avverso il presente provvedimento sono ammessi i seguenti ricorsi:
   - opposizione al Presidente, entro il periodo di pubblicazione, da parte di ogni cittadino ai sensi dell'art. 183, comma 5 del Codice degli Enti locali della Regione Autonoma Trentino - Alto Adige, approvato con Legge regionale 3 maggio 2018, n. 2;
   - ricorso giurisdizionale avanti al Tribunale Regionale Giustizia Amministrativa di Trento, entro 60 giorni, ai sensi degli artt. 13 e 29 del D.Lgs. 2 luglio 2010, n. 104;
   - ricorso straordinario al Presidente della Repubblica, entro 120 giorni, ai sensi dell'art. 8 del D.P.R. 24 novembre 1971, n. 1199;

   richiamando per gli atti delle procedure di affidamento relativi a pubblici lavori, servizi o forniture, ivi comprese le procedure di affidamento di incarichi di progettazione e di attività tecnico - amministrative ad esse connesse, la tutela processuale di cui agli artt. 119 e 120 del D.Lgs. 2 luglio 2010, n. 104, per effetto della quale il ricorso al Tribunale Regionale Giustizia Amministrativa di Trento va proposto entro 30 giorni e non è ammesso il ricorso straordinario al Presidente della Repubblica.

Data lettura del presente decreto, lo stesso viene approvato e sottoscritto.

IL PRESIDENTE	IL SEGRETARIO GENERALE
Andrea Fontanari	dott.ssa Mariuccia Cemin

Documento prodotto in originale informatico e firmato digitalmente ai sensi degli art. 20 e 21 del "Codice dell'amministrazione digitale" (D.Leg.vo 82/2005).

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

Documento approvato con deliberazione del Comitato esecutivo n. 29 di data 11.03.2019 e revisionata con decreto del Presidente n. _____ di data _____		
Revisione	Data	Motivo
1.0	Data decreto	• Modificato il pt. 4: indicata avvenuta nomina del referente data breach • Aggiornato il pt. 6: notifica della violazione all'Autorità Garante

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, in ossequio alle previsioni di cui agli artt. 33 e 34 del Regolamento europeo n. 679 del 2016.

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, propone al Segretario generale della Comunità l'aggiornamento della presente procedura e la sottopone all'approvazione dell'Organo competente affinché la renda esecutiva.

3 Definizioni

Le seguenti definizioni dei termini utilizzati in questo documento sono tratte dall'art. 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'art. 51 del GDPR dell'UE.

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

Il Titolare, con atto di nomina di data 13/03/2019, ha nominato l'Amministratore di Sistema ed il Referente della gestione delle violazioni dei dati personali, di seguito semplicemente denominato "Referente data breach", individuati nella figura del tecnico informatico dell'Ente.

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 Priovacy 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";
- condividere con il Referente privacy e il Titolare i risultati dell'indagine;
- riferire i risultati dell'indagine al Responsabile della Protezione dei Dati inviando il "Modello di potenziale violazione di dati personali al Responsabile Protezione Dati" compilato all'indirizzo serviziorpd@comunitrentini.it.

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.

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 di quanto disposto dall'art. 33 del Regolamento (UE) 2016/679.

Comunità Alta Valsugana e Bersntol

PROCEDURA DATA BREACH

REGISTRO DELLE VIOLAZIONI

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

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 _____