CITTÀ DI VENTIMIGLIA

(PROVINCIA DI IMPERIA)

VERBALE DI DELIBERAZIONE
DELLA GIUNTA COMUNALE

n. 125 del 11/08/2025

OGGETTO: APPROVAZIONE DELLA PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) AI SENSI DEL REGOLAMENTO (UE) N. 679/2016.

L'anno **duemilaventicinque addì undici del mese di Agosto** alle ore 12:00 nella solita sala delle riunioni della Residenza Municipale, in seguito a regolare convocazione avvenuta nei modi e nei termini di legge, si è riunita la Giunta Comunale nelle persone dei Signori:

N.	Cognome e Nome		Presente	Assente
1	DI MURO FLAVIO	Sindaco	X	
2	AGOSTA MARCO	Vice Sindaco	X	
3	CALCOPIETRO SERENA	Assessore	X	
4	CALIMERA DOMENICO	Assessore	X	
5	CATALANO ADRIANO	Assessore	X in videoconferenza	
6	RACO MILENA	Assessore	X	

Partecipa in qualità di Segretario Verbalizzante il Vice Segretario Generale Paola Savina Elisa Marcheselli il quale provvede alla redazione del presente verbale. Essendo legale il numero degli intervenuti il Sindaco Flavio Di Muro assume la presidenza e dichiara aperta la seduta per la trattazione dell'oggetto indicato.

Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa

LA GIUNTA COMUNALE

SENTITO il positivo indirizzo politico-amministrativo dell'Assessore competente nel rispetto delle linee programmatiche del mandato per il periodo 2023-2028 e degli obiettivi strategici contenuti nel Documento Unico di Programmazione 2025/2027;

PREMESSO CHE:

- la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale e sia l'articolo 8, comma 1, della Carta dei diritti fondamentali dell'Unione Europea ("Carta"), sia l'articolo 16, comma 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 Comune di Ventimiglia, in quanto Titolare del trattamento, è tenuto pertanto a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (*data breach*), incluse eventuali notifiche all'Autorità di controllo competente ed eventuali comunicazioni agli interessati;

VISTI:

- il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati, di seguito "Regolamento");
- il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, così come modificato dal decreto legislativo 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 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» (di seguito "Codice");
- il decreto legislativo 18 maggio 2018, n. 51, recante Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (di seguito "d.lgs. n. 51/2018");
- le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018;

Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa

- la *Opinion 5/2019 on the interplay between the ePrivacy Directive and the RGPD, in particular regarding the competence, tasks and powers of data protection authorities*, adottata, ai sensi dell'art. 64 del Regolamento, dal Comitato europeo per la protezione dei dati in data 12 marzo 2019;
- il Provvedimento del Garante sulla notifica delle violazioni dei dati personali (*data breach*) - 30 luglio 2019;

CONSIDERATO CHE:

- in caso di violazione dei dati personali, il Titolare del trattamento è tenuto a notificare tale evento al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (artt. 33 e 55 del Regolamento, art. 2-bis del Codice);
- il Titolare del trattamento è tenuto altresì a notificare la violazione dei dati personali al Garante con le modalità di cui all'art. 33 del Regolamento anche con riferimento al trattamento effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvo che il trattamento medesimo sia effettuato dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero (artt. 26 e 37, comma 6, del d.lgs. n. 51/2018);
- per «violazione dei dati personali» (*data breach*) si intende 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 (art. 4, punto 12 del Regolamento; art. 2, comma 1, lett. m, del d.lgs. n. 51/2018);
- per la omessa notifica di *data breach* all'Autorità di controllo o per l'omessa comunicazione agli interessati o per entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 del RGPD, sono previste pesanti sanzioni amministrative (art. 83 del RGPD), il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato totale annuo dell'esercizio precedente, se superiore, nonché le misure correttive di cui all'art. 58 del RGPD (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati);
- inoltre, l'art. 82 prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del RGPD ha il diritto di ottenere il risarcimento del danno dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile);
- lo stesso RGPD, all'art. 83 paragrafo 2, indica dei fattori che possono mitigare o aggravare la violazione e, tra questi, un elemento che può sicuramente mitigare il livello sanzionatorio, a fronte di una violazione, è legato al comportamento del Titolare che possa dimostrare come, intervenendo con tempismo, abbia fatto il possibile per ridurre la gravità, la natura e la durata della violazione. L'atteggiamento reattivo e cooperativo comporta, inoltre, un'attenuazione delle sanzioni applicabili;

RITENUTO pertanto:

Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa

a) di fondamentale importanza predisporre una procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette, di dati personali per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l'Ente (*data breach policy*). A tale riguardo si precisa che, presso il Titolare, sono già state attivate procedure a tutela della sicurezza dei dati, tra cui:

   - l'adozione di misure organizzative e tecniche per garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati personali e alle altre informazioni trattate, comprese misure volte al tempestivo ripristino della disponibilità in caso di incidente sulla sicurezza;
   - l'organizzazione, a cadenza periodica, di corsi di formazione per i dipendenti/collaboratori sui principi cardine della normativa sul trattamento dati, sulla sicurezza dei dati personali e dei sistemi;
   - la predisposizione di un sistema di protezione, mediante apposite misure tecniche (es. *firewall*, antivirus) dell'accesso ad internet e ai dispositivi elettronici;

b) strategico per il Comune:

   - sensibilizzare il personale in ordine alle responsabilità in materia di protezione dei dati personali ed all'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli incidenti sulla sicurezza (inclusi i *data breach*);
   - definire processi per identificare, tracciare e reagire ad un incidente sulla sicurezza e ad un *data breach*, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di *data breach*, si renda necessario procedere alla notifica al Garante e alla comunicazione agli Interessati;
   - definire ruoli e responsabilità per la risposta agli incidenti sulla sicurezza ed i *data breach*;
   - assicurare un adeguato flusso comunicativo all'interno della struttura del Titolare tra le parti interessate;
   - stabilire che le procedure contemplate nell'approvando documento siano applicabili a tutte le attività svolte dal Titolare, con particolare riferimento alla gestione di tutti gli archivi e documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati, anche con il supporto di fornitori esterni;
   - stabilire che il rispetto dell'adottanda procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia. In particolare, le procedure medesime sono rivolte a tutti i soggetti che, a qualsiasi titolo, trattano dati personali di competenza del Titolare, quali:

     I. i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto contrattuale intercorrente - abbiano accesso ai dati personali trattati nel corso delle prestazioni rese all'interno della struttura

Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa

organizzativa del Titolare del trattamento;

II. qualsiasi soggetto (persona fisica o persona giuridica) diverso da quelli indicati alla lettera precedente che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 del RGPD);

VISTO il Decreto del Sindaco n. 6 del 15/01/2025, con il quale è stato designato l'avv. Massimo Ramello quale Responsabile della Protezione dei Dati Personali (DPO) per il Comune di Ventimiglia, nel rispetto della vigente normativa;

VISTA l'allegata procedura per la gestione della violazione dei dati personali (*data breach*), concordata con il sopra nominato DPO, 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;

RITENUTA la predetta procedura, con i relativi allegati, meritevole di approvazione;

VISTO il Decreto Legislativo – 18/08/2000, n. 267 – Testo unico delle leggi sull'ordinamento degli enti locali;

VISTO il vigente Statuto dell'Ente;

VISTO il regolamento sul funzionamento della Giunta Comunale approvato con DGC n. 65 del 31/03/2022;

VISTO il Documento Unico di Programmazione – DUP 2025/2027, approvato dal Consiglio Comunale con la deliberazione n. 88 del 27/12/2024, dichiarata immediatamente esecutiva;

VISTA la deliberazione del Consiglio Comunale n. 89 del 27/12/2024 con la quale è stato approvato il Bilancio di Previsione 2025/2027, dichiarata immediatamente esecutiva;

VISTA la deliberazione di Giunta Comunale n. 3 del 13/01/2025, di approvazione e di assegnazione del P.E.G. 2025/2027, dichiarata immediatamente esecutiva;

ACQUISITI i pareri favorevoli di cui agli artt. 49 e 147 bis del D.lgs. 267/2000 alla presente allegati, espressi per la regolarità tecnica e contabile dal Segretario generale Dott.ssa Monica

Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa

Veziano;

tutto ciò premesso, con voti unanimi favorevoli legalmente espressi

DELIBERA

1) DI APPROVARE, per i motivi sopra indicati e qui integralmente richiamati, l'allegata procedura per la gestione della violazione dei dati personali (*data breach*), concordata con il DPO del Comune di Ventimiglia, richiesta dagli articoli 33 e 34 del RGPD "Regolamento Generale sulla Protezione dei Dati" (Regolamento UE 2016/679), come descritta e riportata nel documento – comprendente anche i moduli allo stesso allegati – che si acclude alla presente deliberazione, di cui costituisce parte integrante e sostanziale;

2) DI DARE ATTO che tale procedura contiene le indicazioni, le responsabilità e le azioni da attivare in caso di una 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 ed in ossequio alle previsioni di cui agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016;

3) DI DISPORRE che il presente provvedimento venga inviato ai Dirigenti e ai funzionari E.Q. e che ne venga assicurata la massima diffusione presso tutto il personale operante presso il Comune (Amministratori, Dipendenti, Collaboratori) e presso tutti i soggetti esterni alla struttura organizzativa comunale, qualificabili come Contitolari o Responsabili del trattamento;

4) DI DARE ATTO che le disposizioni operative sono soggette a revisione da parte del Titolare del Trattamento ogni qualvolta si renderà necessario senza necessità di ulteriore formale approvazione da parte della Giunta Comunale;

5) DI DISPORRE CHE al presente provvedimento venga assicurata la pubblicità legale con pubblicazione all'Albo Pretorio, nonché la trasparenza mediante la pubblicazione sul sito *web* istituzionale, nella sezione "Amministrazione trasparente", sotto sezione "Altri contenuti-Privacy".

SUCCESSIVAMENTE, su proposta del Presidente

LA GIUNTA COMUNALE

ATTESA, inoltre, l'urgenza di dare esecuzione al presente provvedimento, per approntare

Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa

tempestivamente la procedura per la gestione della violazione dei dati personali (*data breach*) del Comune di Ventimiglia;

VISTO l'art. 134, comma 4, del Testo Unico delle Leggi sull'ordinamento degli Enti Locali, approvato con D. Lgs 18/08/2000 n. 267;

A VOTI unanimi favorevoli legalmente espressi

DELIBERA

DI DICHIARARE la presente deliberazione immediatamente eseguibile, ai sensi dell'art. 134, comma 4, del D.lgs. 267/2000.

Letto, confermato e sottoscritto digitalmente.

Il Vice Segretario	**Il Sindaco**
Paola Savina Elisa Marcheselli / InfoCert S.p.A.	*FLAVIO DI MURO / ARUBAPEC S.P.A.*

Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa