COMUNE DI PIEVE EMANUELE

Città Metropolitana di Milano

Via Viquarterio, n. 1 – 20072 Pieve Emanuele - Cod. Fisc. 80104290152 – P. IVA 04239310156 - Tel.:02 907881-
sito: **www.comune.pieveemanuele.mi.it** **PEC: protocollo@pec.comune.pieveemanuele.mi.it**

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE N° 115 del 15/10/2025

OGGETTO: APPROVAZIONE DEL DOCUMENTO DI " VALUTAZIONE DI IMPATTO SUL TRATTAMENTO DEI DATI PERSONALI RELATIVI AL SISTEMA DI VIDEOSORVEGLIANZA IN DOTAZIONE AL CORPO INTERCOMUNALE DI POLIZIA LOCALE DEI COMUNI DI PIEVE EMANUELE E SIZIANO"

L'anno duemilaventicinque addì quindici del mese di Ottobre a partire dalle ore 15:30, nella sala giunta del Palazzo Municipale, in seguito ad apposita convocazione avvenuta secondo le forme e le modalità previste dallo statuto e dalla normativa vigente, si è riunita la Giunta Comunale.

In seguito ad appello nominale risultano essere presenti:

N°	Qualifica	Nome	Presente	Assente
1	SINDACO	COSTANZO PIERLUIGI	X	
2	VICE SINDACA	PAOLETTI ERMINIA MARIA	X	
3	ASSESSORE	ROGLIANI EUGENIO	X	
4	ASSESSORE	RAPPOCCIOLO GIOVANNI	X	
5	ASSESSORA	MAZZUOCCOLO MARGHERITA ALMERINDA	X	
6	ASSESSORA	POLITO VALENTINA GIUSY		X

PRESENTI: 5 ASSENTI: 1

Partecipa alla seduta, ai sensi di quanto disposto dall'art. 97 del d.lgs. n. 267/2000 e s. m. e i. e dunque con funzioni consultive, referenti e di assistenza agli organi il Segretario Comunale Salvatore Pagano.

Il Sig.Pierluigi Costanzo, nella sua qualità di Sindaco presiede il collegio; indi, dopo aver constatato la sussistenza del quorum strutturale, dichiara aperta la seduta e pone in discussione il punto, inserito all'odierno ordine del giorno.

In seguito ad ampio ed esaustivo dibattito,

LA GIUNTA COMUNALE

Approvazione del documento di "Valutazione di impatto sul trattamento dei dati personali relativi al sistema di videosorveglianza in dotazione al Corpo Intercomunale di Polizia Locale dei comuni di Pieve Emanuele e Siziano"

Premesso che:
- il Comune di Pieve Emanuele, con Delibera di Consiglio Comunale n. 9 del 01/03/2021, esecutiva ai sensi di legge;
- il Comune di Siziano, con Delibera di Consiglio Comunale n. 3 del 04/03/2021, esecutiva ai sensi di legge;
  hanno manifestato la volontà di gestire le funzioni di Polizia Municipale e Polizia Amministrativa Locale in forma associata ai sensi dell'articolo 30 del D.Lgs. 267/2000 e che in data 18/12/2017 è stata sottoscritta la *"Convenzione tra i comuni di Pieve Emanuele e Siziano per la gestione in forma associata delle funzioni di Polizia Municipale e Polizia Amministrativa Locale – ex articolo 30 del D.Lgs. 267/2000"*;
- con DGC 56/2021 del Comune di Pieve Emanuele e DGC 70/2021 del comune di Siziano è stato approvato il "Regolamento del Corpo Intercomunale di Polizia Locale" dei comuni di Pieve Emanuele e Siziano;
- con DCC 34/2021 del Comune di Pieve Emanuele è stato approvato il "Regolamento per la disciplina della videosorveglianza del comune di Pieve Emanuele";
- con DCC 9/2022 del comune di Siziano è stato approvato il "Regolamento per la disciplina della videosorveglianza del comune di Siziano";
- il sistema di videosorveglianza installato sui territori di Pieve Emanuele e Siziano è gestito presso la Centrale Operativa del Comando del Corpo Intercomunale di Polizia Locale dei comuni di Pieve Emanuele e Siziano;

Rilevato che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale e che 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;

Considerato che le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche, tenuto conto che la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali in considerazione, in particolare, di quanto segue:
- la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo;
- la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono

disponibili al pubblico su scala mondiale informazioni personali che li riguardano;
- la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali;

Tenuto presente che tale evoluzione ha indotto l'Unione Europea ad adottare 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 e che abroga la direttiva 95/46/CE (di seguito solo "GDPR");

Dato atto che il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, il quale è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;

Rilevato che, con il GDPR, è stato richiesto agli Stati membri un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;

Visto il D. lgs 196/2003, modificato dal D.Lgs. 10 agosto 2018 n. 101;

Dato atto che, quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il GDPR obbliga i titolari a svolgere:
- una "determinazione preliminare della possibilità che il trattamento possa presentare un rischio elevato" in base alla quale stabilire se un trattamento può, anche solo teoricamente, presentare un rischio elevato;
- una valutazione di impatto nel caso in cui la determinazione preliminare restituisca l'accertamento della teorica possibilità che il trattamento possa presentare un rischio elevato;

Tenuto presente che la DPIA è una procedura prevista dall'Art. 35 del Regolamento UE 206/679 (RGDP) che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli;

Tenuto presente l'obbligo, in capo ai Titolari, di consultare l'Autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l'impatto del trattamento non siano sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato;

Rilevato che la DPIA deve essere condotta prima di procedere al trattamento e che, deve comunque essere previsto un riesame continuo della DPIA, ripetendo la valutazione a intervalli regolari;

Dato atto che la responsabilità della DPIA spetta al Titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata ad un altro soggetto, interno o esterno all'organizzazione;

Tenuto presente che, ferma restando la discrezionalità dell'Amministrazione nell'effettuare la determinazione preliminare e la valutazione di impatto, il Garante, con provvedimento n. 467 del 11 ottobre 2018, ha reso pubblico l'elenco delle tipologie di trattamenti da sottoporre obbligatoriamente a valutazione d'impatto, tra cui si menzionano:

1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad *"aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"*;
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono *"effetti giuridici"* oppure che incidono *"in modo analogo significativamente"* sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi);
3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.;
4. Trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti);
5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8);
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo);
7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e

testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01;
8. Trattamenti che comportano Io scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment);
10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Tenuto presente che, ai sensi dell'art. 29 delle linee guida elaborate dal Gruppo di Lavoro 29 per la protezione dei dati, la DPIA, non è necessaria per i trattamenti che:
- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto, e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti per la cui definizione è stata una DPIA;

Rilevato che, per quanto sopra, è necessario istituire:
1. una "Determinazione preliminare della possibilità che il trattamento possa presentare un rischio elevato" in base alla quale stabilire se un trattamento può, anche solo teoricamente, presentare un rischio elevato;
2. una valutazione di impatto nel caso in cui la determinazione preliminare restituisca l'accertamento della teorica possibilità che il trattamento possa presentare un rischio elevato;

Dato atto che il Titolare del trattamento dei dati tramite sistemi di videosorveglianza, al fine di garantire la massima diffusione interna ed esterna e la massima conoscibilità dei trattamenti oggetto di DPIA, nonché delle misure tecniche e organizzative individuate dai titolari per mitigare l'impatto del trattamento, è tenuto a garantire la conoscibilità della Valutazione d'impatto sulla protezione dei dati (DPIA) a tutti i dipendenti dell'Ente;

Visti:
il Regolamento (UE) n. 679/2016;

le Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
le Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
le Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
le Linee-guida per l'individuazione dell'Autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
le Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
le Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
le Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e pro lazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
le Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo dl lavoro Art. 29 il 6 febbraio 2018;
il Parere del WP29 sulla limitazione della finalità 13/EN WP 203;

Vista la propria competenza a deliberare in merito a norma del combinato disposto degli articoli 42 e 48 del D.Lgs 267/2000;

VISTO lo statuto comunale ed il ROUS;

VISTO il d.lgs. n. 267/2000 e s.m.i.;

ACQUISITO il parere favorevole espresso dal Titolare di E.Q. dell'Area Sicurezza e Polizia Locale in ordine alla mera regolarità tecnica, ai sensi dell'art. 49 comma 1, del d.lgs. n. 267/2000 e s. m. e i.;

DATO ATTO che l'adozione del presente atto non comporta impegno di spesa e/o riduzione di entrata e che quindi non necessita acquisire l'attestazione di copertura finanziaria ai sensi dell'art. 151, comma 4, del D. Lgs n. 267/2000 e s.m.i;

Con votazione unanime e favorevole espressa nei modi di legge

DELIBERA

1. di recepire ed approvare quanto espresso in premessa che forma parte integrante e sostanziale del presente atto;

2. di approvare la "Valutazione di impatto sul trattamento dei dati personali relativi al sistema di videosorveglianza in dotazione al Corpo Intercomunale di

Polizia Locale dei comuni di Pieve Emanuele e Siziano" ai sensi del Regolamento (UE) n. 679/2016, allegata alla presente, per formarne parte integrante e sostanziale;

3. di trasmettere la presente deliberazione all'Ufficio Affari Generali per:
   la pubblicazione all'Albo Pretorio e sul sito istituzionale dell'Ente,
   la trasmissione a tutto il personale dipendente ed al DPO.

Con successiva e separata votazione, la Giunta, all'unanimità, dichiara la presente deliberazione immediatamente eseguibile, ai sensi dell'art. 134, comma 4, del D. Lgs. 18 agosto 2000, n.° 267 e ss. mm. ed ii.

Letto, confermato e sottoscritto

Il Sindaco	Il Segretario Comunale
Pierluigi Costanzo	Salvatore Pagano

(atto sottoscritto digitalmente)