COMUNE DI SANTA MARIA A VICO

Provincia di Caserta

VERBALE DI DELIBERAZIONE DEL CONSIGLIO COMUNALE

DATA: 19-04-2021
N° DELIBERA: 11

OGGETTO: APPROVAZIONE NUOVO REGOLAMENTO PER LA DISCIPLINA ED UTILIZZO DEGLI IMPIANTI DI VIDEOSORVEGLIANZA.

L'anno duemilaventuno addì diciannove del mese di Aprile alle ore 18:10, previo invito, si è riunito il Consiglio Comunale, in seduta a distanza ai sensi del decreto del Presidente del Consiglio Comunale n.1 del 20.03.2020,in seduta ordinaria,nelle persone dei signori:

Componente	Presente	Assente
PIROZZI ANDREA	X	
BIONDO VERONICA	X	
CIOFFI ANNA	X	
GRIECO ROSSELLA	X	
NUZZO GIUSEPPE	X	
VIGLIOTTI VINCENZO	X	
AFFINITA CLEMENTE	X	
DE LUCIA CARMINE	X	
MONIELLO VINCENZO	X	
FERRARA MARCANTONIO	X	

Componente	Presente	Assente
DE LUCIA CARMINE	X	
PASCARELLA TIZIANA	X	
CRISCI PASQUALE	X	
SIGNORIELLO CLELIA	X	
DE LUCIA FRANCESCO	X	
PISCITELLI CESARE	X	
NUZZO IGINO	X	

La seduta si svolge convenzionalmente presso la sede istituzionale del Comune;
Tutti i componenti ed il Segretario Generale sono collegati in video e audio conferenza tramite il programma Microsoft Teams;

Presiede il sig.**CARMINE DE LUCIA**.

Partecipa alla seduta **il Segretario Generale -** Dott.ssa Claudia Filomena Iollo

Il Presidente dichiara aperta la seduta, dopo aver constatato la sussistenza del numero legale. Invita i Consiglieri Comunali a trattare, discutere e definire l'argomento all'ordine del giorno.

11) Approvazione Regolamento per la disciplina del sistema di Videosorveglianza sul territorio comunale;

Componenti	Pres.	Ass.

PIROZZI ANDREA – Sindaco	X	
BIONDO VERONICA	X	
CIOFFI ANNA	X	
GRIECO ROSSELLA	X	
NUZZO GIUSEPPE	X	
VIGLIOTTI VINCENZO	X	
AFFINITA CLEMENTE	X	
DE LUCIA CARMINE 73	X	
MONIELLO VINCENZO	X	
FERRARA MARCANTONIO	X	
DE LUCIA CARMINE 58	X	
PASCARELLA TIZIANA	X	
CRISCI PASQUALE	X	
SIGNORIELLO CLELIA	X	
DE LUCIA FRANCESCO	X	
NUZZO IGINO	X	
PISCITELLI CESARE	X	

Totale presenti n. 17; Totali assenti n. 0

Il Presidente dà la parola al Consigliere Giuseppe Nuzzo che evidenzia l'importanza del regolamento proposto al consiglio per l'approvazione. Il Consigliere ricorda che il Comune ha circa 100 telecamere collocate sul territorio per cui è stato necessario dotarsi di un regolamento aggiornato che garantisca al meglio la tutela dei dati personali oggetti di trattamento.

Chiede e riceve la parola il Consigliere Crisci che preannuncia il voto favorevole del suo gruppo condividendo il contenuto del regolamento e chiede di valutare la possibilità di trattenere le immagini per più di sette giorni consentendo ai privati di accedere alle telecamere.

Il Consigliere Giuseppe Nuzzo precisa che non è possibile trattenere le immagini per più di sette giorni e che il regolamento prevede la possibilità dei privati di convenzionarsi.

Concluso l'intervento il Presidente pone ai voti la proposta ad oggetto "Approvazione Regolamento per la disciplina del sistema di Videosorveglianza sul territorio comunale".

IL CONSIGLIO COMUNALE

Esaminata l'allegata proposta di deliberazione;

Ritenuto la stessa sufficientemente motivata e condividendo e facendo proprio senza riserve il contenuto della medesima, al quale integralmente si rimanda anche per quanto riguarda i riferimenti normativi.

Visto i pareri espressi ai sensi dell'art. 49 comma 1° e art. 147 bis comma 1 del D.Lgs. 267/2000 dai Responsabili di Servizio in ordine alla regolarità tecnica e contabile.

Con voti favorevoli unanimi espressi per alzata di mano

D E L I B E R A

Di approvare la proposta di deliberazione che forma parte integrante e sostanziale del presente provvedimento.

Il Sindaco propone al Consiglio Comunale l'approvazione del Regolamento che segue :

CONSIDERATO che questo Comune è dotato di un impianto di videosorveglianza in alcune parti del territorio comunale, volto alla tutela della sicurezza urbana ed alla prevenzione e repressione dei reati;
RICHIAMATA la propria Delibera di C.C. n. 85 del 05.10.2009 con la quale si approvava il Regolamento per l'utilizzo degli impianti di videosorveglianza;
CONSIDERATO che i trattamenti dei dati personali nell'ambito di una attività di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti previsti dal citato codice in materia di protezione dei dati personali, nonché i provvedimenti emessi dal Garante per la protezione dei dati personali;

VISTO che il Regolamento UE n. 2016/679 ha varato il nuovo "*Pacchetto Europeo protezione dati*" che disciplina i nuovi rapporti con le Pubbliche Amministrazioni e le imprese e che abroga la direttiva la Direttiva 95/46/Ce in materia di protezione dei dati personali/privacy, entrata in vigore l'8 maggio 1997.

VISTO che la *Direttiva (UE) 2016/680* del Parlamento europeo e del Consiglio, del 27 aprile 2016, disciplina la 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.

VISTO il D.lgs 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679 del Parlamento

Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
CONSIDERATO quindi opportuno e necessario procedere all'adeguamento del vigente regolamento e, pertanto, procedere all'adozione di un provvedimento che disciplini complessivamente l'utilizzo delle apparecchiature audiovisive per garantire l'accertamento degli illeciti, nel rispetto dei diritti e delle libertà fondamentali dei cittadini e della dignità delle persone, con particolare riferimento alla riservatezza, all'identità ed alla protezione dei dati personali;
ACQUISITO il previsto parere da parte del DPO/RPD che testualmente si riporta *"considerato il trattamento posto in essere e le sue finalità di interesse pubblico e preso atto della probabilità e gravità dei rischi e le libertà degli interessati, il titolare del trattamento ha individuato idonee prassi e misure volte all'attenuazione del rischio capaci di garantire la sicurezza dei sistemi ed il pieno esercizio dei diritti ed il godimento delle libertà delle persone. i trattamenti andranno revisionati (ed eventualmente aggiornati) almeno con cadenza annuale, salvo variazioni significative dei trattamenti"*
RILEVATO che la bozza di regolamento in argomento è stata approvata all'unanimità dalla Commissione regolamenti di questo Ente in data 1.4.2021 ,come risulta dal relativo verbale di seduta;

PROPONE DI DELIBERARE

1) **DI APPROVARE** il Regolamento Comunale per la Disciplina ed utilizzo degli impianti di videosorveglianza, che consta di n.25 articoli e n . 7 allegati, che viene accluso al presente atto per costituirne parte integrante e sostanziale.
2) **DI ABROGARE** il precedente Regolamento per l'utilizzo degli impianti di videosorveglianza, approvato con Delibera di Consiglio Comunale C.C. n. 85 del 5.10.2009
3) **DI INVIARE** il regolamento medesimo alla Prefettura di Caserta.
Lì 2.4.2021

IL SINDACO
-Andrea PIROZZI –

ADEGUAMENTO REGOLAMENTO PER LA DISCIPLINA DEL SISTEMA DI VIDEOSORVEGLIANZA SUL TERRITORIO COMUNALE

INDICE

CAPO I – PRINCIPI GENERALI

Art. 1 – Oggetto e ambito di applicazione

1. Il presente Regolamento disciplina le operazioni di modalità di trattamento dei dati personali mediante sistemi di videosorveglianza adottati dal Comune di Santa Maria a Vico, gestiti nell'ambito del proprio territorio, nel rispetto di quanto previsto dal Provvedimento del garante per la Protezione dei dati personali in materia di videosorveglianza del 08 aprile 2010 e le Linee Guida n. 3/2019 sul trattamento dei dati personali attraverso la videosorveglianza adottate dal European Data Protection Board (E.D.P.D.).
2. Costituisce videosorveglianza quel complesso di strumenti finalizzati alla vigilanza in remoto, cioè che si realizza a distanza mediante dispositivi di ripresa video, captazione di immagini eventuale conseguente analisi, collegati a un centro di controllo e coordinamento direttamente gestito dal Comando di Polizia Locale.
3. Con il presente Regolamento si garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di sistemi di videosorveglianza gestiti e impiegati dal Comune nel proprio territorio, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, in applicazione del Regolamento UE n. 679/2016 (di seguito GDPR) e del D.lgs. n. 196/2003 così come modificato dal D.lgs. n. 101/2018 (di seguito Codice Privacy).

4. Il trattamento dei dati mediante sistemi di videosorveglianza svolti dal Comune di Santa Maria a Vico in qualità di titolare del trattamento nonché "autorità compente" ai fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro la prevenzione di minacce alla sicurezza pubblica sarà effettuato in applicazione del D.lgs. n. 51/2018.

Art. 2 – Definizioni

1. Ai fini del presente regolamento si applicano le seguenti definizioni:
   1. **«dati personali»:** qualsiasi informazione riguardante una persona fisica identificata o identificabile, **(«interessato»)**; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, in particolare con 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 dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica;
   2. **«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;
   3. **«limitazione di trattamento»:** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
   4. **«profilazione»:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
   5. **«pseudonimizzazione»:** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile;
   6. **«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;
   7. **«autorità competente»:**
      a) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica;
      b) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica;
   8. **«titolare del trattamento»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o dello Stato membro, il titolare del trattamento o i criteri specifici applicabili alla sua nomina possono essere previsti dal diritto dell'Unione o dello Stato membro. **Ai sensi dell'art. 4 paragrafo 7 del Regolamento U.E. n. 679/2016 (GDPR) il Comune di SANTA MARIA A VICO è il Titolare del Trattamento;**
   9. **«responsabile del trattamento»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
   10. «**persone autorizzate**»: le persone fisiche alle quali il titolare o il responsabile del trattamento attribuiscono specifici compiti e funzioni connesse al trattamento dei dati personali e operano sotto la loro autorità;
   11. **«destinatario»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione europea o dello Stato membro non sono considerate destinatari; il trattamento di tali dati da parte di tali autorità pubbliche è conforme alle norme in materia di protezione dei dati applicabili secondo le finalità del trattamento;
   12. **«violazione dei dati personali»:** la violazione della 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;
13. **«file di log»:** registro degli accessi e delle operazioni;
14. **«categorie particolari di dati»:** dati personali che rilevino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
15. **«Forze di polizia»:** le Forze di Polizia di cui all'articolo 16 della legge 1° aprile 1981, n. 121;
16. **«Forze di polizia locale»:** di cui alla legge 7 marzo 1986 n. 65;
17. **«blocco»:** la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
18. **«dato anonimo»:** il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
19. **«comunicazione»:** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal responsabile e dalle persone autorizzate ai sensi dell'art. 2 quaterdecies, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
20. **«diffusione»:** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

Art. 3 – Principi applicabili al trattamento di dati personali

1. Le norme del presente Regolamento si fondano sui principi previsti dall'art. 5 del GDPR e dall'art. 3 del D.lgs. 51/2018 ed in particolare:

a) **Liceità, correttezza e trasparenza**: il trattamento di dati personali effettuato attraverso sistemi di videosorveglianza da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali. Esso infatti è necessario per l'esecuzione di un obbligo di legge, un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui i Comuni sono investiti.

b) **Limitazione della finalità**: i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non siano incompatibili con tali finalità. Sono considerate compatibili le finalità di archiviazione nel pubblico interesse, ricerca scientifica o storica ai fini statistici e per i trattamenti di cui al D.lgs. 51/2018, in caso di finalità differenti saranno compatibili solo se conformi a quanto stabilito dall'ordinamento interno o dall'Unione europea.

c) **Minimizzazione**: i sistemi di videosorveglianza sono configurati per l'utilizzazione al minimo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

d) **Esattezza**: esatti e se necessario aggiornati, devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

e) **Limitazione della conservazione**: conservati con modalità che consentono l'identificazione degli interessati per il tempo necessario al conseguimento delle finalità per le quali sono trattati, sono sottoposti a esame periodico per verificarne la persistente necessità di conservazione, successivamente cancellati o anonimizzati una volta corso tale termine. Risulta compatibile la conservazione per archiviazione nel pubblico interesse e ricerca scientifica o storica ai fini statistici;

f) **Integrità e riservatezza**: trattati in modo da garantire un'adeguata sicurezza e protezione mediante misure tecniche ed organizzative adeguate rispetto a trattamenti non autorizzati o illeciti ed alla perdita, distruzione o danno accidentale.

2. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché, dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Comune di Santa Maria a Vico mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente ai principi suindicati.

Art. 4 – Base Giuridica e Finalità

1.Le basi giuridiche e le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza sono conformi alle funzioni istituzionali attribuite al Comune di SANTA MARIA A VICO. Secondo quanto previsto dall'art. 2-ter del Codice della privacy la base giuridica per il trattamento dei dati personali

effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui all'art. 6 paragrafo 3 lettera b) del GDPR è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamenti.
2.Il trattamento è lecito in quanto ricorrono le seguenti basi giuridiche:

- D.P.R. 24 luglio 1977, n. 616;
- Legge 24 novembre 1981, n. 689;
- Legge 7 marzo 1986, n. 65 – Legge Quadro Polizia Locale;
- D.lgs. 18 agosto 2000, n. 267 – T.U.E.L.
- D.L. 92/2008 convertito con Legge n. 125 del 24/07/2008;
- D.M. 5 agosto 2008 – Ministero del Lavoro;
- Circolare n. 558/SICPART/421.2/70 – anno 2012 – Ministero dell'Interno;
- D.L. 20 febbraio 2017, n. 14 come convertito dalla Legge 18 aprile 2017, n. 48;
- D.L. 23 febbraio 2009, n. 11;
- Linee Guida "Piattaforma della Videosorveglianza integrata";
- Linee Guida per l'attuazione della sicurezza urbana – art. 5 della Legge n. 48/2017;
- Linee Generali delle Politiche pubbliche per la promozione della sicurezza integrata;
- Decreto del Presidente della Repubblica n. 15 del 15 gennaio 2018;
- D.lgs. 3 aprile del 2006 n. 152, e successivi;
- Legge 22 maggio del 2015, n. 68;
- Codice procedura penale e codice penale;

3.L'utilizzo dei sistemi di videosorveglianza è finalizzato alla tutela della sicurezza urbana nei luoghi pubblici o aperti, per l'adozione di atti e iniziative in materia di ordine e sicurezza pubblica, ed ai fini di prevenzione, indagine, accertamento e perseguimento di reati, (tra cui rientra la tutela della sicurezza ambientale) o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, a norma del D.lgs. n. 51/2018. Un ulteriore finalità è la tutela della sicurezza stradale per monitorare la circolazione lungo le strade del territorio comunale e fornire ausilio in materia di polizia amministrativa in generale.
4.Il sistema di videosorveglianza implica il trattamento di dati personali che possono essere rilevati da telecamere tradizionali eventualmente munite di algoritmi di analisi video, metadati, conteggio delle persone e verifica dei comportamenti o varchi lettura targhe connessi a black list in grado di verificare in tempo reale la regolarità della sosta e di un transito di un veicolo.
5.La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui al successivo articolo 9 del presente regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa solo se prevista ai sensi del comma 1. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.
6.La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1.

Art. 5 – Partenariato Pubblico – Privato

1.Il Comune di SANTA MARIA A VICO promuove e attua, per la parte di competenza, politiche di controllo del territorio integrate con organi istituzionalmente preposti alla tutela della sicurezza e dell'ordine pubblico. A tal fine il Comune, previa intesa o su richiesta delle autorità di pubblica sicurezza o degli organi di polizia, può consentire l'utilizzo delle registrazioni video degli impianti comunali di videosorveglianza, con le modalità di cui all'articolo precedente. In attuazione e promozione della sicurezza integrata il Comune può stipulare accordi o patti con autorità di pubblica sicurezza o organi di polizia (patti per l'attuazione della sicurezza urbana di cui all'art. 5 Legge 48/2017) per l'utilizzo e condivisione di sistemi di videosorveglianza, in tal caso dovrà essere stipulato un accordo di contitolarità secondo quanto previsto dal successivo comma 3 dell'art. 6 del presente regolamento.
2.Il Comune di SANTA MARIA A VICO promuove, per quanto di propria competenza, il

coinvolgimento dei privati per la realizzazione di singoli impianti di videosorveglianza, orientati comunque su aree o strade pubbliche o a uso pubblico, nel rispetto dei principi di cui al presente Regolamento, previa valutazione di idoneità dei siti e dei dispositivi. I privati interessati assumono su di sé ogni onere per acquistare le attrezzature e renderle operative, con connessione al sistema centrale, in conformità alle caratteristiche tecniche dell'impianto pubblico. Gli interessati mettono gli impianti a disposizione dell'Ente a titolo gratuito, senza mantenere alcun titolo di ingerenza sulle immagini e sulla tecnologia connessa, previa stipula di apposita convenzione **(Allegato A).** Il Comune assume su di sé gli oneri per la manutenzione periodica e la responsabilità della gestione dei dati raccolti.

CAPO II – IL TRATTAMENTO DEI DATI PERSONALI

Art. 6 – Il Titolare del Trattamento

1.Il Titolare del trattamento dei dati raccolti mediante il sistema di videosorveglianza è il Comune di SANTA MARIA A VICO. Anche per le attività di Polizia così come previste dal D.lgs. n. 51/2018 il Comune di SANTA MARIA A VICO in qualità di autorità competente è il Titolare del Trattamento dei dati personali. La centrale operativa è installata presso il Comando di Polizia Municipale e il Comandante della Polizia Municipale o suo delegato vigila sull'utilizzo dei sistemi, sul trattamento delle immagini e dei dati in conformità agli scopi indicati nel presente Regolamento e alle altre disposizioni normative che disciplinano la materia.
2.Il Comune di SANTA MARIA A VICO ha provveduto ai sensi dell'art. 37 del GDPR alla nomina del Responsabile della Protezione dei Dati personali il quale svolgerà i compiti previsti dall'art. 39 del GDPR e dell'art. 28 del D.lgs. 51/2018, fungendo da punto di contatto con il Garante e con gli interessati.
3.Qualora due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento dovranno stipulare un accordo interno di contitolarità che determini in modo trasparente le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento e dalla normativa comunitaria in tema di protezione dei dati personali.
4.Il Comandante individua e nomina, con proprio provvedimento, nell'ambito degli appartenenti al Comando di Polizia Locale, le persone autorizzate della gestione dell'impianto nel numero ritenuto sufficiente a garantire la corretta gestione del servizio di videosorveglianza.
5.Con l'atto di nomina, ai singoli autorizzati sono affidati compiti e funzioni specifici e le puntuali prescrizioni per l'utilizzo dei sistemi, nel rispetto dall'art. 29 del GDPR e art. 2-quaterdecies del Codice Privacy.

Art. 7 – Informazioni sul trattamento dei dati personali

1. I soggetti interessati che stanno per accedere in una zona videosorvegliata, devono essere informati mediante appositi cartelli sul trattamento di dati personali attraverso la videosorveglianza **(ALLEGATO B e B1**).
2.Sul sito istituzionale del Comune di SANTA MARIA A VICO sono pubblicate le informazioni obbligatorie da fornire agli interessati per il trattamento dei dati personali attraverso i sistemi di videosorveglianza secondo quanto previsto dall'art. 13 del GDPR e dall'art. 10 del D.lgs. 51/2018 **(ALLEGATO C).**

Art. 8 – Modalità di raccolta dei dati

1. I dati personali sono raccolti attraverso riprese video e captazione di immagini effettuate da sistemi di telecamere installate in luoghi pubblici ed aperti al pubblico, nonché in immobili di proprietà comunale e perimetrali ad esso, ubicati nel territorio di competenza.
2. Le telecamere di cui al precedente comma consentono riprese video a colori o in bianco e nero, possono essere dotate di brandeggio e di zoom ottico e sono collegate alla centrale operativa del Comando di Polizia Municipale, che potrà, esclusivamente per il perseguimento dei fini istituzionali, eventualmente digitalizzare o indicizzare le immagini.
3. I segnali video delle unità di ripresa sono visionabili presso la Centrale Operativa ubicata presso il Comando di Polizia Municipale, sotto la responsabilità del Comandante o di un suo delegato.
4. Come stabilito dall'art. 21 del D.lgs. 51/2018 le operazioni di raccolta, modifica, consultazione, comunicazione, trasferimento, interconnessione e cancellazione di dati, eseguite in sistemi di trattamento automatizzati, sono registrate in appositi file log, da conservare per la durata stabilita dal Decreto del Presidente della Repubblica n. 15/2018. Le registrazioni devono consentire di conoscere i

motivi, la data e l'ora di tali operazioni e, se possibile, di identificare la persona che ha eseguito le operazioni e i destinatati. Inoltre, saranno utilizzate solo per la verifica della liceità del trattamento, per finalità di controllo e per garantire la sicurezza ed integrità dei dati e nell'ambito di procedimenti penali. Saranno messi a disposizione del Garante su richiesta.

Art. 9 – Categorie particolari di dati e dati personali relativi a condanne penali e reati

1.Il trattamento dei dati attraverso sistemi di videosorveglianza non sempre deve essere considerato come un trattamento di categorie particolari di dati. Se le immagini sono elaborate per ricavare categorie particolari di dati si applica l'art. 9 del GDPR che vieta il trattamento di tali dati personali prevedendo delle eccezioni al secondo paragrafo. Anche nei casi in cui non si applica l'articolo 9 paragrafo 1 del GDPR, il Titolare del trattamento dei dati deve sempre cercare di ridurre al minimo il rischio di acquisire immagini che rivelino altri dati particolari indipendentemente dalla finalità prevista. Ogni volta che si installa un sistema di videosorveglianza si deve prestare particolare attenzione al principio di minimizzazione dei dati.
2.I trattamenti delle categorie particolari di dati personali di cui all'art. 9 del GDPR necessari per motivi di interesse pubblico rilevante sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutela i diritti fondamentali e gli interessi dell'interessato. Le materie in cui si considera rilevante l'interesse pubblico sono elencate all'art. 2-sexies del D.lgs. 196/2003.
3.Per quanto riguarda le finalità previste dal D.lgs. n. 51/2018 l'art. 7 prevede che il trattamento dei dati di cui all'art. 9 del GDPR è autorizzato solo se strettamente necessario e assistito da garanzie adeguate per i diritti e libertà dell'interessato e specificamente previsto dal diritto dell'Unione europea o da legge, o nei casi previsti dalla legge, da regolamento, ovvero, ferme le garanzie dei diritti e delle libertà, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato.
4.Il trattamento dei dati personali relativi a condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6 paragrafo 1 del GDPR che non avviene sotto il controllo dell'autorità pubblica, è consentito, ai sensi dell'art. 10 del GDPR solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati, fatti salvi i casi di applicazione del D.lgs. n. 51/2018.

Art. 10 – Conservazione dei dati personali

1.Le immagini videoregistrate sono conservate per un tempo non superiore a 7 giorni nella centrale di registrazione, e nel rispetto del principio di limitazione della conservazione. Al termine del periodo stabilito il sistema di videoregistrazione provvede in automatico alla loro cancellazione - ove tecnicamente possibile - mediante sovra-registrazione, con modalità tali da rendere non più utilizzabili i dati cancellati.
2.La conservazione delle immagini oltre il termine fissato dal precedente comma è consentita esclusivamente per speciali esigenze investigative di polizia giudiziaria con particolare riferimento ai varchi lettura targhe e ad altre esigenze correlate all'attività di istituto, comunque per il tempo strettamente necessario alla conclusione del relativo procedimento amministrativo.
3.Con decreto del Presidente della Repubblica, adottato ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, sono individuati, per i trattamenti o le categorie di trattamenti non occasionali di cui al comma 1, i termini, ove non già stabiliti da disposizioni di legge o di regolamento, e le modalità di conservazione dei dati, i soggetti legittimati ad accedervi, le condizioni di accesso, le modalità di consultazione, nonché le modalità e le condizioni per l'esercizio dei diritti di cui agli articoli 9, 10, 11 e 13. I termini di conservazione sono determinati in conformità ai criteri indicati all'articolo 3, comma 1, tenendo conto delle diverse categorie di interessati e delle finalità perseguite.

Art. 11 – Individuazione dei siti da sottoporre a videosorveglianza

1.L'individuazione o variazione dei luoghi da sottoporre a videosorveglianza nel rispetto dell'art. 4 "Base giuridica e Finalità" del presente regolamento, compete alla Giunta Comunale con apposita deliberazione.
2 Alla Giunta Comunale compete inoltre l'autorizzazione, sempre nel rispetto dei principi e delle finalità del presente regolamento, all'utilizzo dei sistemi di videosorveglianza mobili dotati di sistemi di registrazione autonomi ed alimentazione anche a batteria e/o celle solari, o di altro genere, a

supporto delle attività di prevenzione e di accertamento delle violazioni commesse nell'ambito delle competenze della Polizia Municipale fatto salvo l'eventuale utilizzo per le finalità di Polizia Giudiziaria, anche con la direzione e coordinamento dell'Autorità Giudiziaria.

Art. 12 - Utilizzo di particolari sistemi mobili.

A) Body Cam e Dash Cam

1. Gli operatori della Polizia Municipale possono essere dotati nello svolgimento di servizi operativi e di controllo del territorio delle Body Cam (ossia sistemi di ripresa indossabili) e delle Dash Cam (telecamere a bordo veicoli di servizio) in conformità delle indicazioni dettate dal Garante della Privacy con nota 26 luglio 2016, prot. n. 49612, con cui sono state impartite le prescrizioni generali di utilizzo dei predetti dispositivi il cui trattamento dei dati è ricondotto nell'ambito del D.lgs. 51/2018 trattandosi di "dati personali direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela all'ordine e della sicurezza pubblica, nonché di polizia giudiziaria".
Il Comandante curerà la predisposizione di uno specifico disciplinare tecnico interno, da somministrare agli operatori di Polizia Municipale che saranno dotati di microcamere, con specificazione dei casi in cui le microcamere devono essere attivate, dei soggetti autorizzati a disporre l'attivazione, delle operazioni autorizzate nel caso di emergenza e di ogni altra misura organizzativa e tecnologica necessaria alla corretta e legittima gestione dei dispositivi e dei dati trattati.
2. Le videocamere e le schede di memoria di cui sono dotati i sistemi di cui al comma precedente dovranno essere contraddistinte da un numero seriale che dovrà essere annotato in apposito registro recante il giorno, l'orario, i dati indicativi del servizio e la qualifica e nominativo del dipendente che firmerà la presa in carico e la restituzione.
La scheda di memoria, all'atto della consegna ai singoli operatori, non dovrà contenere alcun dato archiviato.
Il sistema di registrazione dovrà essere attivato solo in caso di effettiva necessità, ossia nel caso di insorgenza delle situazioni descritte dal disciplinare tecnico interno.
3. Il trattamento dei dati personali effettuati con simili sistemi di ripresa devono rispettare le disposizioni del presente regolamento: in particolare i dati personali oggetto di trattamento debbono essere pertinenti, completi e non eccedenti le finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, per poi essere cancellati, nel rispetto del precedente articolo 10.

B) Telecamere modulari e riposizionabili (foto trappole – telecamere semimobili)

7. Il Comando di Polizia Municipale può dotarsi di telecamere riposizionabili, anche del tipo foto-trappola, con generazione di allarmi da remoto per il monitoraggio attivo.
8. Le modalità di impiego dei dispositivi in questione saranno disciplinate con apposito provvedimento prima dell'uso.
9. Gli apparati di videosorveglianza modulare riposizionabili vengono installati secondo necessità, nei luoghi teatro di illeciti penali; possono essere utilizzati per accertare illeciti amministrativi, solo qualora non siano altrimenti accertabili con le ordinarie metodologie di indagine. Qualora non sussistano finalità di sicurezza o necessità di indagine previste dal D.lgs. 51/2018 che esimono il Titolare dall'obbligo di informazione, si provvederà alla previa collocazione della adeguata cartellonistica, per l'informativa agli utenti frequentatori di dette aree.
10. In ogni caso le modalità di trattamento e di conservazione dovranno rispettare quanto indicato dall'art. 10 del presente regolamento, nonché quanto disposto dalla vigente normativa.

C) Uso dei sistemi aereo mobili a pilotaggio remoto (SAPR)

11. Il Comando di Polizia Municipale, per lo svolgimento delle attività di competenza può dotarsi di ogni altra tecnologia di ripresa video e di captazione di immagini necessaria al raggiungimento delle finalità istituzionali.
12. In particolare può dotarsi di Sistemi Aeromobili a Pilotaggio Remoto – droni – sia per l'esecuzione di riprese ai fini di tutela della sicurezza urbana, sia per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali ,di sistemi di rilevamento automatizzati delle infrazioni al codice della strada e/o di supporto alle attività di accertamento del personale di Polizia Municipale (rilevamento a strascico di violazioni mediante video ,foto ecc che riprendano anche immagini di contesto rispetto alle violazioni rilevate, ecc.)
13. In ogni caso, i dispositivi e il loro utilizzo devono essere conformi alla normativa vigente, con

particolare riferimento alla regolamentazione adottata dall'Ente Nazionale per l'Aviazione Civile e al Codice della Navigazione per quanto concerne i droni.
14. In ogni caso le modalità di trattamento e di conservazione dovranno rispettare quanto indicato dall'art. 10 del presente regolamento, nonché quanto disposto dalla vigente normativa.

Art. 13 – Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali

1.Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento è il responsabile del trattamento rispettano le condizioni di cui al capo V del GDPR, fatte salve le altre disposizioni dello stesso. Tutte le disposizioni del capo V del GDPR sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato.
2.Il D.lgs. n. 51/2018 dagli articoli dal 31 al 36 del Capo IV disciplina i principi generali in materia di trasferimento di dati personali.

CAPO III – DIRITTI DELL'INTERESSATO

Art. 14 – Diritto di accesso dell'interessato

1. Il titolare del trattamento non deve in alcuni casi distribuire le immagini in cui è possibile identificare altri soggetti, ma deve implementare misure tecniche per soddisfare la richiesta di accesso.
2. In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza specifica, in riferimento al tempo ed in proporzione alla quantità di soggetti registrati nell'area monitorata, ha diritto:

a) di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e di ottenere l'accesso ai dati;
b) di ottenere informazioni sulle finalità del trattamento, le categorie di dati personali in questione, i destinati o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
c) di ottenere quando possibile, il periodo di conservazione o il criterio per determinarlo;
d) di ottenere le informazioni relative all'esistenza del diritto di chiedere al titolare del trattamento il blocco dei dati qualora essi siano trattati in violazione di legge;
e) diritto di proporre reclamo ad un'autorità di controllo;
f) di ottenere informazioni relativi all'esistenza di un processo decisionale automatizzato compresa la profilazione ed all'esistenza di adeguate garanzie nel caso di trasferimenti in paesi terzi;

3. In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo.
4. Il titolare del trattamento oltre all'obbligo di cancellare i dati personali in caso di richiesta dell'interessato è tenuto in base ai principi del GDPR a limitare i dati personali memorizzati. Sfocare l'immagine senza alcuna capacità retroattiva di recuperare i dati personali dell'immagine precedentemente contenuta equivale alla cancellazione dei dati in conformità del GDPR.
5. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione, secondo quanto previsto dall'art. 2 – terdecies del Codice Privacy.
6. Il diritto di accesso è fatto salvo i limiti previsti dall'art. 23 del GDPR, art. 2 – undecies del Codice della Privacy e dell'art. 14 del D.lgs. n. 51/2018.
7. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento, in caso di richieste eccessive o manifestatamente infondate è possibile addebitare un costo ragionevole.
8. Le istanze sono presentate al Titolare del Trattamento o al Responsabile della Protezione dei dati secondo il modello allegato al presente regolamento (**ALLEGATO D**).

CAPO IV – LE MISURE DI SICUREZZA DEI DATI PERSONALI

Art. 15– Misure tecniche ed organizzative

1.Il Titolare del Trattamento deve adottare misure tecniche ed organizzative proporzionali ai rischi per i diritti e le libertà delle persone fisiche, derivanti da distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso ai dati di videosorveglianza. Ai sensi degli art. 24 e 25 del GDPR il Titolare del Trattamento deve attuare misure tecniche ed organizzative anche per salvaguardare tutti i principi di protezione dei dati durante il trattamento e stabile i mezzi affinché gli interessati possano esercitare i propri diritti come definiti nel presente regolamento.
2.Il Titolare dovrà adottare un quadro interno e le politiche che possano garantire tale attuazione sia al momento della determinazione dei mezzi per il trattamento si al momento del trattamento stesso, compresa la fase della valutazione di impatto sulla protezione dei dati, quando necessario.
3.Tenendo conto dello state dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà degli interessati, il Comune adotta le seguenti misure:

a) La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
b) La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
c) Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

4.Chiunque agisce sotto l'autorità del Titolare del Trattamento non tratta tali dati se non è istruito in tal senso.
5.In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante per la protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, rispettando le indicazioni previste dall'art. 33 del GDPR. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati, il titolare del trattamento comunica la violazione all'interessato senza giustificato motivo. Il modello per la notifica è allegato al presente regolamento **(ALLEGATO F).**

Art. 16 - Sicurezza dei dati

1. I dati personali oggetto di trattamento sono conservati presso la centrale di registrazione individuata, alla quale può accedere il solo personale autorizzato secondo istruzioni che devono essere impartite dal Comandante della Polizia Municipale.
2. In particolare l'accesso agli ambienti in cui è ubicata una postazione di controllo è consentito solamente al personale in servizio presso il Corpo di Polizia Municipale autorizzato dal Comandante. Il Comandante della Polizia Municipale impartisce idonee istruzioni atte ad evitare assunzioni o rilevamento di dati da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali.
3. Il personale autorizzato, istruito secondo quanto previsto dal comma 6 dell'art. 6 del presente regolamento, andrà nominato tra gli Ufficiali ed Agenti in possesso della qualifica di agenti di Pubblica Sicurezza in Servizio presso il Settore di Polizia Municipale e nei vari settori operativi del Corpo di Polizia Municipale che, per esperienza, capacità ed affidabilità, forniscono idonea garanzia nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.
4. Le operazioni di trattamento di sistemi di videosorveglianza aventi per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali è riservata al personale della Polizia Municipale, aventi qualifica di Ufficiali ed Agenti di Polizia Giudiziaria ai sensi dell'art. 55 del codice di procedura penale, istruito nelle modalità di cui al precedente comma e come previsto dall'art. 19 del D.lgs. 51/2018.
5. In ogni caso, prima dell'utilizzo degli impianti, tutto il personale sarà istruito al corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento.
6. Le persone autorizzate al trattamento saranno dotati di proprie credenziali di autenticazione di accesso al sistema registrati mediante apposti file di log, anche come previsto dall'art. 21 del D.lgs. n. 51/2018.

Art. 17 – Misure di sicurezza specifiche

1. Per le operazioni di trattamento svolte per le finalità di cui al D.lgs. n. 51/2018, previa valutazione dei rischi, vengono adottate le misure tecniche ed organizzative previste dall'art. 25 del D.lgs. 51/2018 volte a:
a) vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);

b) impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);
c) impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);
d) impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»);
e) garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);
f) garantire la possibilità di individuare i soggetti ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);
g) garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);
h) impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);
i) garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);
l) garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).

Art. 18 - Valutazione d'impatto

1.Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologiche, considerati la natura, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.
2.La sorveglianza sistematica su larga scala di una zona accessibile al pubblico richiede una valutazione d'impatto sulla protezione dei dati personali, secondo le modalità di cui all'art. 35 del GDPR. Pertanto, il titolare del trattamento provvede, pertanto, allo sviluppo di una valutazione d'impatto, costantemente aggiornata, effettuata ai sensi dell'art. 35 del GDPR, adottando misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati. **(ALLEGATO F)**

CAPO V – TUTELA AMMINISTRATIVA, GIURISIDIZIONALE E PENALE

Art. 19 – Tutela amministrativa e giurisdizionale

1. L'interessato qualora ritenga che i diritti di cui gode sulla base della normativa in materia di protezione dei dati personali siano stati violati può proporre reclamo al Garante o ricorso dinanzi all'autorità giudiziaria secondo quanto previsto dall'art. 140 bis del Codice della Privacy.
2. L'interessato può rivolgersi al Garante mediante reclamo ai sensi dell'art. 77 del GDPR secondo le modalità previste dal Capo I – Tutela dinnanzi al Garante del Codice della Privacy.
3. Tutte le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli articoli 78 e 79 del GDPR e quelli comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali, nonché il diritto al risarcimento del danno ai sensi dell'articolo 82 del GDPR, sono attribuite all'autorità ordinaria.
4. Per i trattamenti svolti in applicazione del D.lgs. n. 51/2018 sono previsti rimedi amministrativi e giurisdizionali in favore dell'interessato dagli art. 37 a 42 – Capo V Tutela e sanzioni amministrative.

Art. 20 – Violazioni e sanzioni amministrative

1.Qualora il trattamento dei dati personali attraverso sistemi di videosorveglianza costituisca una violazione delle disposizioni e/o inosservanza dei principi previsti dal GDPR e dal Codice della

Privacy, i criteri di applicazione delle sanzioni amministrative pecuniarie ed il procedimento di adozione dei provvedimenti corretti e sanzionatori sono disciplinati dall'art. 166 del Codice Privacy.
2.Le disposizioni relative a sanzioni amministrative previste dal Codice della Privacy e dall'art. 83 del GDPR non si applicano in relazione ai trattamenti svolti in ambito giudiziario.
3.Salvo che il fatto costituisca reato e ad esclusione dei trattamenti svolti in ambito giudiziari l'art. 42 del D.lgs. n. 51/2018 prevede due differenti ipotesi di sanzioni amministrative in caso di violazioni di specifiche disposizioni previste dal D.lgs. n. 51/2018.

Art. 21 – Illeciti penali

1.Determinate condotte messe in atto per effettuare operazioni di trattamento dei dati personali possono costituire idonei presupposti per la determinazione di un illecito penale.
2.Il Capo II – Illeciti penali del Codice della Privacy individua una serie di condotte penalmente rilevanti di seguito elencate:
- Art. 167 – Trattamento illecito di dati;
- Art. 167 bis – Comunicazione e diffusione di dati personali oggetto di trattamento su larga scala;
- Art. 167 ter – Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala;
- Art. 168 – Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio di poteri del Garante;
- Art. 170 – Inosservanza di provvedimenti del Garante;
- Art. 171 – Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori;
- Art. 172 – Pene accessori;

2.Il Capo VI – Illeciti penali del D.lgs. n. 51/2018 individua una serie di condotte penalmente rilevanti di seguito elencate:
- Art. 43 – Trattamento illecito di dati;
- Art. 44 -Falsità in atti e dichiarazione al Garante;
- Art. 45 – Inosservanza di provvedimenti del Garante;
- Art. 46 – Pene accessorie.

CAPO VI – DISPOSIZIONI INTEGRATIVE SUI TRATTAMENTI DELLE FORZE DI POLIZIA

Art. 22 – Modalità di trattamento e flussi di dati da parte delle Forze di polizia

1.Nei casi in cui le autorità di pubblica sicurezza o le Forze di polizia possono acquisire in conformità alle vigenti disposizioni di legge o di regolamento dati raccolti mediante sistemi di videosorveglianza, l'acquisizione può essere effettuata anche per via telematica. A tal fine gli organi o uffici interessati possono avvalersi di convenzioni volte ad agevolare la consultazione da parte dei medesimi organi o uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei principi di cui agli articoli da 3 a 8 del D.lgs. 51/2018. Le convenzioni-tipo sono adottate dal Ministero dell'interno, su conforme parere del Garante, e stabiliscono le modalità dei collegamenti e degli accessi anche al fine di assicurare l'accesso selettivo ai soli dati necessari al perseguimento delle finalità di cui all'articolo 1, comma 2 del D.lgs 51/2018.
2. I dati trattati dalle Forze di polizia per le finalità di cui al D.lgs n. 51/2018, sono conservati separatamente da quelli registrati per finalità amministrative che non richiedono il loro utilizzo.

Art. 23 – Tutela dell'interessato

1.Restano ferme le disposizioni di cui all'articolo 10, commi 3, 4 e 5, della legge 1° aprile 1981, n. 121, e successive modificazioni, concernenti i controlli sul Centro elaborazione dati del Dipartimento della pubblica sicurezza.
2.Le disposizioni di cui all'articolo 10, commi 3, 4 e 5, della legge n. 121 del 1981, si applicano, oltre ai dati destinati a confluire nel Centro elaborazione dati di cui al comma 1, ai dati trattati con l'ausilio di strumenti elettronici da organi, uffici o comandi delle Forze di polizia di cui all'articolo 16 della predetta legge n. 121 del 1981.

CAPO VII – NORME FINALI

Art. 24 – Modifiche regolamentari e rinvio

1.I Contenuti del presente regolamento, ove necessario, dovranno essere adeguati o quanto meno interpretati alla luce delle modifiche legislative italiane e comunitarie, provvedimenti ed opinioni del Garante per la protezione dei dati e dell'E.D.P.B. intervenute successivamente all'entrate in vigore del presente regolamento e da ritenersi immediatamente recepite in via recettizia.
2.Per tutto quanto non disciplinato nel presente regolamento si rinvia alle norme del GDPR, del Codice della Privacy e del D.lgs. n. 51/2018, nonché al provvedimento del Garante per la protezione dei dati in materia di videosorveglianza del 08 aprile 2010 ed alle Linee Guida dell'E.D.P.B. n. 3/2019 sul trattamento dei dati personali attraverso videosorveglianza.

Art. 25 - Decorrenza e abrogazioni

1. Il presente regolamento entra in vigore contestualmente con l'esecutività della relativa Delibera di approvazione e comporta l'immediata abrogazione del precedente regolamento adottato con deliberazione di Consiglio Comunale del 5.10.2009 n. 85

- ALLEGATO A – CONVENZIONE PRIVATI
- ALLEGATO B e B1 – INFORMATIVA CARTELLI
- ALLEGATO C – INFORMATIVA DETTAGLIATA
- ALLEGATO D – MODALITA' ESERCIZIO DIRITTI
- ALLEGATO E – NOTIFICA DATA BREACH
- ALLEGATO F – VALUTAZIONE D'IMPATTO
- ALLEGATO G – PROCEDURA PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

Deliberazione n. 11 del 19-04-2021

Letto, confermato e sottoscritto.

Il Presidente del Consiglio
Ing. CARMINE DE LUCIA

Il Segretario Generale
Dott.ssa Claudia Filomena Iollo

[X] Deliberazione dichiarata immediatamente eseguibile ai sensi dell' art. 134, comma 4, del D.Lgs. 267/2000 e.ss.mm.ii.

[ ] Deliberazione esecutiva ad ogni effetto di legge decorso il decimo giorno di pubblicazione, ai sensi dell'art. 134, comma 3, del D.Lgs n. 267/2000 e.ss.mm.ii.

Il Segretario Generale

Documento informatico sottoscritto con firma digitale ai sensi dell'art.24 del D.Lgs. n.82/2005 e ss.mm.ii.

Copia del documento informatico formato e depositato presso questo Ente.