Comune di Mandello del Lario
Provincia di Lecco

REGOLAMENTO COMUNALE PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA URBANA INTEGRATA SUL TERRITORIO COMUNALE

Approvato dal Consiglio Comunale con deliberazione n. ..53..... in data ..21/12../2022....

SOMMARIO/INDICE.

Capo I - principi generali……pag.4
PREMESSA……pag.4
Art. 1 - Oggetto del regolamento…… pag.4
Art. 2 - Definizioni……pag.5
Art. 3 - Finalità e sistemi di videosorveglianza e base giuridica……..pag.7
Art. 4 - Ambito di validità e di applicazione del presente regolamento. Gestione delle funzioni di polizia locale associate/convenzionate…….. pag.8
Art. 5 - Principi generali……pag.9
Art. 6 - Trattamento e acquisizione dei dati personali – Scuole – traffico - emergenze……pag.9

Capo II - Soggetti coinvolti nel trattamento……pag.11
Art. 7 - Titolare del trattamento……pag.11
Art. 8 - Designato (supervisore) e Autorizzato……..pag.11
Art. 9 - Nomina, compiti e funzioni del "Designato"……pag.11
Art 10 - Nomina, compiti e funzioni degli "Autorizzati"…….. pag.12
Art. 11 - Persone autorizzate ad accedere fisicamente ai sistemi e ai luoghi……pag 13
Art. 12 - Soggetti esterni che trattano dati per conto del Titolare……..pag.14
Art. 13 - Amministratori di Sistema. Responsabili esterni del trattamento - gestione tecnica degli impianti di videosorveglianza……...pag.14
Art. 14 - Soggetti autorizzati al trattamento e preposti alla gestione dell'impianto di videosorveglianza.. pag15

Capo III - Trattamento dei dati personali……pag.16
Art. 15 - Diretta visione delle immagini - acquisizione dati……..pag.16
Art. 16 - Modalità di raccolta e requisiti dei dati personali -Scelta e luoghi d'installazione apparati - Tempi di conservazione……...pag.16
Art. 17 - Modalità da adottare per i dati video ripresi. Accesso ai sistemi ed alle immagini……...pag.17
Art. 18 - Comunicazione - Sicurezza nelle trasmissioni……..pag.18
Art. 19 - Limiti alla utilizzabilità di dati personali……pag.19
Art. 20 - Tipi di trattamenti autorizzati – video e vocali……pag.19

Capo IV - Diritti degli interessati……pag.20
Art. 21 - Informativa……pag.20
Art. 22 - Diritti dell'interessato……...pag.21

Capo V - Misure di sicurezza…..……pag.22
Art. 23 - Criteri e modalità di estrazione delle immagini richieste……pag.22
Art. 24 - Ottemperanza al Provvedimento del 27/11/08 del Garante per la protezione dei dati personali relativo al controllo dell'operato degli amministratori di sistema..……pag.22
Art. 25 - Requisiti minimi sul luogo di collocazione del server……pag.22
Art. 26 - Requisiti minimi sugli strumenti elettronici, informatici e telematici……pag.23
Art. 27 - Obblighi degli autorizzati……pag.23
Art. 28 - Sicurezza dei dati ……pag.23
Art. 29 - Cessazione del trattamento dei dati ……pag.24
Art. 30 - Trasmissione dei video - audio……pag.24

Capo VI - Accesso ai dati da parte di altri soggetti…… ……pag.25
Art. 31 - Accordi con enti pubblici e privati……pag.25
Art. 32 - Accesso ai dati da parte delle Forze di Polizia (art. 16 L. 121/81), Polizia Locale e dell'Autorità Giudiziaria……pag.25
Art. 33 - Accesso telematico da parte delle Autorità Giudiziarie. ……pag.25
Art. 34 - Accesso da parte di privati o loro delegati – altri servizi interni o Enti esterni……pag.25

Capo VII - Dispositivi di videosorveglianza …… ……pag.28
Art. 35 - Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada…… pag.28
Art. 36 - Utilizzi particolari - ZTL - A.P. - Centri storici - Z.P.R.U……pag.28
Art. 37 - Abbandono e conferimento dei rifiuti……pag.29

Art.38 - Utilizzo di particolari videocamere mobili: BodyCam, DashCam, dispositivi telefonia mobile. Droni……..pag.29
Art. 39 - Foto trappole ……pag.29
Art. 40 - Utilizzo in ambienti di lavoro…….pag.29

Capo VIII - Gestione del data Breach…… ……pag.30
Art. 41 - Perdita dei dati - Data Breach ……pag.30
Art. 42 - Gestione della comunicazione del data Breach ……pag.30
Art. 43 - Identificazione e indagine preliminare……pag.30
Art. 44 - Contenimento, Recovery e risk assessment……pag.30
Art. 45 - Eventuale notifica all'Autorità Garante competente……pag.31
Art. 46 - Eventuale comunicazione agli interessati. ……pag.31
Art. 47 - Documentazione della violazione……pag.31

Capo IX - Tutela amministrativa e giurisdizionale - Modifiche…… …….pag.32
Art. 48 - Tutela……pag.32
Art. 49 - Modifiche regolamentari - Rinvio dinamico……pag.32
Art. 50 - Danni cagionati per effetto del trattamento di dati personali……pag.32

Capo X - Disposizioni finali…… ……pag.33
Art. 51 - Parternariato pubblico privato per il potenziamento della videosorveglianza ad uso pubblico. Sistemi integrati di trattamento dei dati……pag.33
Art. 52 - Tutela dei dati personali – Valutazione di impianto sulla protezione dei dati……pag.33
Art. 53 - Entrata in vigore…… ……pag.33

CAPO I
PRINCIPI GENERALI

PREMESSA.

I comuni possono utilizzare i sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana (art. 6/c.7 del D.L. n. 11/2009 convertito con L. 38/2009), per curare e difendere il bene pubblico che afferisce alla vivibilità e al decoro del Paese, da perseguire anche attraverso la prevenzione della criminalità, in particolare di tipo "predatorio" (art. 4 del D.L. 14/2017 convertito con L. 48/2017) e per la rilevazione delle violazioni a norme sulla circolazione stradale ("Codice della Strada" D. L.vo 30/4/1992 n. 285 e s.m.i.)

Pertanto i sistemi di videosorveglianza documentano l'attività istituzionale del Comune di Mandello del Lario attraverso le riprese e la registrazione di immagini ovvero mediante la raccolta e la conservazione di informazioni grafiche o audiovisive su tutte le persone che entrano nello spazio monitorato, identificabili in base al loro aspetto o ad altri elementi specifici (paragrafo 2.1delle Linee Guida EDPB - European Data Protection Board - 3/2019).

Art. 1
Oggetto del Regolamento.

1. Il presente regolamento disciplina le modalità di raccolta, gestione e conservazione dei dati personali acquisiti mediante sistemi di videosorveglianza e/o geolocalizzazione ed in generale ogni trattamento dei dati personali effettuato mediante sistemi di acquisizione, registrazione, conservazione e gestione di immagini, audio-immagini, videoriprese e informazioni relative ad esse o alla localizzazione geografica e riguardanti le persone fisiche coinvolte, svolto in forma diretta o indiretta, dal comune di Mandello del Lario, determinandone le modalità di funzionamento e mantenimento, ai sensi di quanto disposto dal D.lgs. n. 196/2003 e ss.mm.ii. (Codice in materia di protezione dei dati personali), Reg. UE n. 2016/679 (Regolamento Generale sulla Protezione dei Dati), D.lgs. n. 51/2018 (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), dal Provvedimento del Garante per la Protezione dei dati personali 8 aprile 2010 (Provvedimento in materia di videosorveglianza), dalle Linee Guida EDPB (European Data Protection Board) n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video adottate il 29/1/2020, dalla L. n. 300/1970 (Statuto dei Lavoratori) e ss.mm.ii., dal DM n. 37/2008 (Disposizioni in materia di attività di installazione degli impianti all'interno degli edifici), dal D.lgs. n. 81/2008 (T.U. in materia di salute e sicurezza nei luoghi di lavoro) e dal D.L. n. 14 del 20 febbraio 2017 convertito in L. n. 48 del 13 aprile 2017 (Disposizioni urgenti in materia di sicurezza delle città).

2. L'installazione e l'attivazione dei sistemi di videosorveglianza non deve essere sottoposta a nessuna autorizzazione da parte del Garante per la Protezione dei dati Personali (G.P.D.P.), ma è sufficiente che il trattamento sia effettuato previa informativa alle persone che stiano per accedere all'area videosorvegliata, utilizzando a tale fine il modello semplificato di informativa predisposto in fac-simile dal Garante per la Protezione dei dati personale, e siano adottate idonee misure di sicurezza.

3. L'installazione e attivazione del Sistema di videosorveglianza integrata con altre Forze di Polizia implica, per la fattiva condivisione delle immagini, la sottoscrizione di un Patto locale per la sicurezza.

4. Le immagini o la geolocalizzazione, qualora rendano le persone identificate o identificabili, costituiscono dati personali. In tali casi detti sistemi incidono sul diritto delle persone alla propria riservatezza.

5. Il presente Regolamento garantisce quindi che la raccolta di informazioni sulle persone identificabili si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

6. Nel territorio del comune di Mandello del Lario sono attivabili impianti di fotosorveglianza e videosorveglianza mobili, posizionabili in aree del territorio comunale individuate dalla Polizia Locale - P.L. - oppure montate su veicoli di servizio, su "droni" (A.P.R. - aeromobili a pilotaggio remoto) da intendersi anche e non solo arerei ma terrestri o acquatici, o indossate dagli stessi operatori di P.L. e utilizzabili per le finalità istituzionali.

7. I sistemi di videosorveglianza comunali possono essere integrati con apparecchiature di rilevazione della targa dei veicoli in transito, installate sui varchi di accesso perimetrali alla rete viaria cittadina, ai fini della sicurezza urbana. La disciplina relativa al trattamento dati di cui al presente Regolamento si applica a tali apparecchi, in quanto, e nei limiti in cui consentano l'acquisizione dei fotogrammi e la registrazione dei dati alfanumerici contenuti nelle targhe dei veicoli.

8. L'utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada, in considerazione della peculiarità dei fini istituzionali perseguiti, non è assoggettato alla disciplina di cui al presente

regolamento, ma alle disposizioni dettate dal Garante della privacy nel Provvedimento del 8 aprile 2010, al paragrafo 5.3 nonché dalla specifica normativa di settore.

9. In particolare, il presente Regolamento:

a) disciplina e definisce le modalità di utilizzo degli impianti di acquisizione immagini, videoriprese e informazioni ad esse relative (es. dati anagrafici, targhe, geolocalizzazione);

b) disciplina e definisce gli adempimenti, le garanzie e le tutele per il legittimo e pertinente trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti.

10. Per tutto quanto non dettagliatamente disciplinato nel presente regolamento, si rinvia a quanto disposto da:

- **D.P.R. n. 15 del 15.01.2018,** recante "*Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia*";
- **Regolamento UE n. 2016/679** 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 indicato con RGPD.
- **Direttiva UE n. 2016/680** del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai 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;
- **D. Lgs. 18/05/2018, 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.".
- **D. Lgs. 30 giugno 2003, n, 196**, come modificato dal D.Lgs. n. 101 del 10 agosto 2018, recante: "Codice in materia di protezione dei dati personali e successive modificazioni; di seguito indicato con Codice.
- Artt. 50 e 54 del **D.Lgs. 18 agosto 2000, n. 267** e s.m.i..
- **Decalogo** del **29 novembre 2000 promosso dal Garante** - GPDP -.
- **Provvedimento** del **29 aprile 2004 del Garante** - GPDP -, ad integrazione ed aggiornamento del decalogo del 29/11/2000.
- **Circolare** del **Ministero dell'Interno** dell'8 febbraio 2005, n. 558/A/471;
- **D. L. 23 febbraio 2009, n. 11**, recante: "Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori ", ed in particolare dall'art. 6;
- **D. L. 20 febbraio 2017 n 14 recante** "Disposizioni urgenti in materia di sicurezza delle città"
- "**Provvedimento in materia di videosorveglianza**" emanato dal garante per la protezione dei dati personali in data 8 aprile 2010;
- **Circolare** del **Ministero dell'Interno** del 2 febbraio 2012, n. 558/SICPART/421.2/70/224632 "Sistemi di videosorveglianza in ambito comunale - Direttiva;
- **Circolare** del **Ministero dell'Interno** del 28 febbraio 2017, n. 0003412 - Prot. uscita del 12 gennaio 2018 n. 0001065 "Realizzazione dei sistemi di lettura targhe ed integrazione al Sistema di Controllo Nazionale Targhe e Transiti (S.C.N.T.T) - Linee di indirizzo.
- **Decreto Ministero dell'Interno del 13/6/22** "modalità di utilizzo da parte delle forze di polizia degli aeromobili a pilotaggio remoto".
- **Linee guida** E.D.P.B. - European Data Protection Board – **del 3/2019** sul trattamento dei dati personali attraverso dispositivi video adottato il 29 gennaio 2020 dal comitato Europeo per la protezione dei dati;
- **Legge 20 maggio 1970 n. 300** - Statuto dei lavoratori -;
- **Circolare** dell'**Ispettorato Nazionale del Lavoro n. 2 del 7/11/2016** - indicazioni si utilizzazione localizzazione GPS veicoli aziendali -;

Art. 2
Definizioni.

1. Ai fini del presente regolamento si intende:

a) per «**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;

b) per «**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;
c) per «**profilazion**e», 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;
d) per «**pseudonimizzazione**», il trattamento dei dati 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 tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
e) per «**titolare del trattamento**», - Ente - Comune di Mandello del Lario -. Secondo l'art. 4 del RGPD è "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 degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
f) per «**responsabile del trattamento**», - Designato o Supervisore - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento; sovrintende l'utilizzo di un sistema di gestione delle informazioni, coordinando le attività dei soggetti autorizzati al trattamento dati;
g) per «**incaricato del trattamento**», - Autorizzato - la persona fisica che abbia accesso a dati personali;
h) per "**interessato**", la persona fisica identificata o identificabile cui si riferiscono i dati personali oggetto di trattamento;
i) per «**terzo**», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
j) per «**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;
k) per «**comunicazione**», il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
l) per "**diffusione**", il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
m) per "**anonimizzazione**" o "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
n) per sistema di "**videosorveglianza**": è un sistema attraverso il quale si effettua la raccolta, la registrazione, la conservazione e in generale l'utilizzo di immagini fotografiche o videoriprese relative a persone fisiche identificate o identificabili, anche indirettamente;
o) Sistema di "**geolocalizzazion**e" è un sistema attraverso il quale si effettua la raccolta, la registrazione, la conservazione e in generale l'utilizzo di informazioni sulla localizzazione geografica relative a persone fisiche identificate o identificabili, anche indirettamente;
p) **D.P.O. (Data Protection Officer)** o **R.P.D.** (**Responsabile Protezione Dati)**: è una figura prevista dall'art. 37 del RGPD. Si tratta di un soggetto designato dal titolare del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Fornisce consulenza sulla necessità o meno di eseguire valutazioni d'impatto sulla protezione dei dati (DPIA), come eseguirle e quali risultati aspettarsi. Coopera con l'Autorità e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali.
Ai fini delle definizioni di cui al presente Regolamento si deve fare riferimento all'art. 4 del RGPD relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e all'art 2 del D. Lgs 51/2018 relativo 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.
q) **C.d.S.** - codice della strada - D. Lvo 30/4/1992 n. 285 e s.m.i.;
r) **Forze di Polizia** come individuate dall'art. 16 della Legge 1/4/1981 n. 121.

s) per "**impianto di videosorveglianza**": qualunque impianto di ripresa, fissa o mobile, composto da una o più telecamere, in grado di riprendere e registrare immagini e suoni, o rilevare le targhe dei veicoli in transito, utilizzato per le finalità indicate nel presente regolamento.
t) per "**impianto di ripresa mobile**": body-cam indossata dall'operatore di Polizia Locale, Dash- Cam installata sui veicoli di servizio, telecamera mobile con lettore targhe.
u) per "**banca dati**": il complesso di dati personali acquisiti mediante l'utilizzo di qualsiasi impianto di videosorveglianza.
v) per "**blocco**": la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.
w) per "**fotogramma**": un'immagine estrapolata da un video oppure un fermo immagine effettuato con la videocamera durante la videoregistrazione della stessa.
x) Per "**droni**" (A.P.R. - aeromobili a pilotaggio remoto) da intendersi apparecchi che si muovono mediante pilotaggio da remoto anche e non solo arerei ma terrestri o acquatici.

Art. 3
Finalità e sistemi di videosorveglianza e base giuridica.

1. . Le finalità di utilizzo degli impianti di videosorveglianza di cui al presente Regolamento sono conformi alle funzioni istituzionali demandate al Comune dalla Legge 7 marzo 1986, n. 65 "Ordinamento della polizia municipale", dalla Legge Regionale n. 6/2015, dallo Statuto e dai Regolamenti comunali, nonché dal D.L. n. 14 del 20 febbraio 2017 convertito in L. n. 48 del 13 aprile 2017 "Disposizioni urgenti in materia di sicurezza delle città" e dalle altre disposizioni normative applicabili al Comune di Mandello del Lario. In particolare, l'uso di impianti di videosorveglianza è strumentale all'attuazione di un sistema integrato di politiche per la sicurezza urbana, di cui alle fonti normative sopra citate.
2. Il presente regolamento garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di impianti di videosorveglianza o geolocalizzazione nel territorio, gestito dal Comune di Mandello del Lario - Servizio di Polizia Locale - che, in prospettiva, potrà anche essere collegato a centrali operative di Forze di Polizia, al Sistema di Controllo Nazionale Targhe e Transiti (S.C.N.T.T) o qualsiasi altro sistema integrato sovracomunale per controlli di polizia, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. Il trattamento dei dati è effettuato per motivi di interesse pubblico rilevanti, finalizzati alla sicurezza della popolazione e alla salvaguardia della vita e dell'incolumità fisica ai sensi dell'art. 2 sexies del D.Lgs. n. 196/03 nonché per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali ai sensi dell'art. 1 comma 2 del n. D.lgs 51/2018. Garantisce altresì i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento. Il sistema informativo e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzati mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
3. Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento. Le finalità perseguite mediante l'attivazione di Sistemi di videosorveglianza sono conformi alle funzioni istituzionali attribuite al Comune di Mandello del Lario, ai sensi dell'art. 6 del D.L. 23/2/09, n. 11, convertito nella Legge 23/4/09 n. 38 ai sensi del quale dispone che "per la tutela della "sicurezza urbana" i Comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico".
4. Per "sicurezza urbana" si intende la tutela della sicurezza pubblica, intesa come attività di prevenzione e repressione dei reati, con esclusione delle funzioni di polizia amministrativa, nonché il bene pubblico che afferisce alla vivibilità ed al decoro delle città. Gli impianti di videosorveglianza installati o in corso di realizzazione dal Comune attengono specificamente ed in via principale alla tutela della sicurezza urbana ed all'eventuale presidio anche delle attività della polizia amministrativa.
5. Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato e finalizzato a:
a) prevenire e reprimere atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" di cui all'articolo 4 del decreto legge n. 14/2017 e delle attribuzioni del Sindaco in qualità di autorità locale di cui all'art. 50 e di ufficiale di governo di cui all'art. 54 comma 4 e 4-bis del D.Lvo 267/2000;
b) prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado, abbandono di rifiuti, inquinamento suolo-acqua-aria, abusi edilizi e svolgere i controlli volti ad accertare e sanzionare le violazioni delle norme contenute nei regolamenti locali in genere e nelle ordinanze sindacali; per le attività di polizia giudiziaria con finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali a norma del D. Lgs. 51/2018;
c) vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;
d) tutelare l'ordine, il decoro e la quiete pubblica;
e) controllare aree specifiche del territorio comunale quali giardini, parchi e simili;

f) tutela del patrimonio comunale, per presidiare gli accessi agli edifici comunali, dall'interno o dall'esterno, e le aree adiacenti o pertinenti ad uffici od immobili comunali
g) monitorare i flussi di traffico e monitorare l'accesso alle zone a traffico limitato; tutela della sicurezza stradale, per monitorare la circolazione lungo le strade del territorio comunale e rilevare le infrazioni connesse al rispetto dei limiti massimi di velocità ammessi - o quant'altro possibile - con apparati appositamente omologati ed ammessi a tale scopo dalle norme, nonché fornire ausilio in materia di polizia amministrativa in generale;
h) verificare e calibrare il sistema di gestione centralizzata degli impianti semaforici ed eventualmente rilevare infrazioni con apparati appositamente omologati ed ammessi dalle norme;
l) registrazione e/o diffusione di sedute di organi collegiali o commissioni, nei casi previsti dalla legge, per assicurare alla cittadinanza pubblicità, trasparenza e massima diffusione sulle attività dell'Ente;
m) tutela del personale della polizia locale mediante apparati indossabili e/o installati su veicoli in dotazione solo per fini e con le modalità ammesse dalle normative vigenti.
6. Nei locali del comando di Polizia Locale potranno essere posizionati monitor per la visione in diretta delle immagini riprese dalle telecamere, laddove ritenuto opportuno e necessario.
7. Ai fini di cui al comma 5 punto g) potranno essere installati sistemi integrati, sistemi intelligenti e sistemi per rilevare violazioni al codice della strada o ad ogni altra norma che preveda la possibilità di rilevare violazioni ai fini della contestazione con sistemi di videosorveglianza e/o geolocalizzazione.
8. L'eventuale utilizzo del sistema di videosorveglianza per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con sistematico accesso da parte di altre forze di polizia e/o di sicurezza, potrà avvenire in seguito a specifica e puntuale richiesta motivata o, nel caso di richiesta di un flusso costante e continuo di dati verso l'autorità giudiziaria, questo dovrà essere specificamente disciplinato con appositi accordi secondo la vigente normativa.
9. A tal riguardo l'Ente potrà altresì promuovere politiche di controllo del territorio integrate con organi istituzionalmente preposti alla tutela della sicurezza e dell'ordine pubblico. Dette politiche di controllo integrato e/o di collaborazione con altri Corpi o Organi preposti alla tutela della sicurezza e dell'ordine pubblico, anche al fine di consentire la visualizzazione diretta delle immagini degli apparati di videosorveglianza, vengono previamente disciplinati con separati accordi in forma scritta (ad esempio con il Sistema di Controllo Nazionale Targhe e Transiti (S.C.N.T.T).
10. Ai fini del presente regolamento per dispositivi di videosorveglianza di cui all'art 2 comma 1 lettera n) si intendono videocamere in postazione fissa, dashcam, bodycam, sistemi di geolocalizzazione, telecamere modulari riposizionabili, droni e quant'altro l'evoluzione tecnologica metterà a disposizione nel tempo.

Art. 4
Ambito di validità e di applicazione del presente regolamento. Gestione delle funzioni di Polizia Locale associate/convenzionate.

1. Le prescrizioni del presente regolamento si applicano obbligatoriamente ai trattamenti di dati personali effettuati tramite sistemi di acquisizione e gestione immagini, audio e videoriprese oltre ad informazioni sulla geolocalizzazione, effettuati mediante sistemi di videosorveglianza acquistati o forniti da terzi posti sotto la diretta titolarità del Comune di Mandello del Lario e/o da altri soggetti in contitolarità all'interno del territorio comunale e con altri Enti convenzionati anche per territori esterni a quello comunale.
2. I dati sono acquisiti tramite strumenti idonei al perseguimento delle finalità istituzionali, attraverso memorizzazione su specifici supporti installati sulle periferiche di acquisizione o trasmissione verso una centrale di acquisizione dei dati.
3. Qualora il servizio di Polizia Locale venga esercitato in forma associata o convenzionata, il Comune capofila o quello in cui vengono conservati e/o raccolti e/o comunque convogliati o trattati i dati rilevati, determinando, congiuntamente agli enti convenzionati, le finalità e le modalità del trattamento, assume il ruolo e le funzioni di titolare del trattamento ed assicura un trattamento dei dati conforme a quanto previsto nel presente Regolamento.
4. Il Comune nel cui territorio vengono rilevati e/o trattati i dati, assume il ruolo di contitolare, autorizza il trattamento ed assume le medesime funzioni per quanto connesso con le attività di installazione, manutenzione, informazione, trasmissione operate sugli impianti di rilevamento e sulla rete di trasmissione.
5. Relativamente al punto precedente, in sede di approvazione, rinnovo o modifica della Convenzione/Associazione per il servizio di Polizia Locale verranno meglio specificate le modalità di rilevazione, conservazione e trattamento dei dati sensibili in modo da renderle omogenee per i Comuni consociati, in aderenza al presente regolamento, anche adottando i medesimi schemi e modelli organizzativi e di gestione.

Art. 5
Principi generali.

1. Il trattamento di videosorveglianza mediante acquisizione di fotografie, video, registrazioni audio e informazioni sulla geolocalizzazione all'interno dell'ambito precedentemente definito si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5 del RGDP e, in particolare:

a) **Principio di liceità** – Il trattamento di dati personali per mezzo di sistemi di videosorveglianza e geolocalizzazione da parte di soggetti pubblici è lecito allorquando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento in ossequio al disposto di cui all'art. 6, paragrafo 1, lett. e) del RGPD. I trattamenti oggetto del presente Regolamento rispondono a detto principio e pertanto sono autorizzati senza necessità di consenso da parte degli interessati.

b) **Principio di necessità** – In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all'art. 5, paragrafo 1, lett. c) del RGPD, i sistemi di acquisizione immagini e videoriprese, i sistemi informativi ed i programmi informatici utilizzati sono configurati per ridurre al minimo l'utilizzazione di dati personali e 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. Pertanto nei sistemi di videosorveglianza è escluso ogni uso superfluo e sono evitati eccessi e ridondanze.

c) **Principio di proporzionalità** – La raccolta e l'uso delle immagini devono essere proporzionati agli scopi perseguiti. In applicazione dei principi di proporzionalità e di necessità, nel procedere alla commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un'effettiva esigenza di deterrenza. A tal riguardo si dà atto che detta valutazione di proporzionalità è stata effettuata dall'Ente su tutto il territorio comunale e che gli impianti di videosorveglianza, laddove previsti, sono stati adottati in quanto altre misure siano state previamente e ponderatamente valutate insufficienti o inattuabili (es. controlli da parte degli operatori di Polizia Locale, posti di blocco effettuati da operatori di polizia locale, sistemi di allarme, misure di protezione degli ingressi). In ogni caso l'Ente garantisce che il trattamento viene effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da controllare e/o da proteggere.

d) **Principio di finalità** – Ai sensi dell'art. 5, paragrafo 1, lett. b) del RGPD, i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. E' consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la sicurezza urbana.

2. Il presente regolamento garantisce che il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza gestiti dal Comune e collegati alle Centrale Operativa del Comando di Polizia Locale si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale come previsti dal Codice e dal GDPR.

3. In attuazione del principio di necessità, gli impianti di videosorveglianza ed i programmi informatici di gestione dello stesso sono configurati in modo tale da ridurre il trattamento di dati personali, in modo da evitare il trattamento quando le finalità perseguite nei singoli casi possono essere raggiunte mediante dati anonimi, o con modalità che permettano di identificare l'interessato solo in caso di necessità.

4. In attuazione del principio di proporzionalità e dei criteri di pertinenza e non eccedenza, gli impianti di videosorveglianza sono configurati in modo da raccogliere esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese ed evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti.

5. A presidio di particolari obiettivi sensibili potranno attivarsi sistemi di telecamere con possibilità di registrare in via continuata, o entrare in funzione, solo in caso di intrusione nell'area pertinenziale di questi, rilevando in automatico comportamenti o eventi anomali e provvedendo o alla segnalazione e registrazione, e, se del caso, azionando un sistema di illuminatori ottici o allarme acustico.

Art. 6
Trattamento e acquisizione dei dati personali – scuole-trafico-emergenze.

1. Il trattamento dei dati personali è effettuato a seguito dell'attivazione di un impianto di videosorveglianza e/o geolocalizzazione.

2. Le finalità istituzionali dei suddetti impianti sono del tutto conformi alle funzioni istituzionali demandate al Comune di Mandello del Lario, in particolare dal D. Lgs. 18 agosto 2000 n. 267, dal D.P.R. 24 luglio 1977 n.

616, dal D. Lgs. 31 marzo 1998 n. 112, dalla legge 7 marzo 1986 n. 65 sull'ordinamento della Polizia Municipale e s.m.i. o sostituzione della stessa, dalla normativa regionale, nonché dallo statuto e dai regolamenti comunali. La disponibilità tempestiva di immagini, suoni o dati di geolocalizzazione presso il comando di Polizia Locale o con appararti portatili/mobili e l'eventuale condivisione con altre forze di polizia costituisce inoltre uno strumento di prevenzione e di razionalizzazione dell'azione della Polizia Locale e delle altre Forze di Polizia.

3. La videosorveglianza/geolocalizzazione effettua una vera e propria attività di vigilanza su persone e beni, sostituendo, in tutto o in parte, la presenza umana sul posto.

4. La risoluzione delle riprese sarà definita in base alle esigenze e, nel caso le telecamere siano state installate per verificare traffico, ingorghi, esondazioni, frane, ecc. potrà anche essere non particolarmente alta. La risoluzione sarà certamente alta per telecamere posizionate ai fini della sicurezza urbana, rilevazione di reati, controllo veicoli o per rilevamento sanzioni quando ciò fosse ammesso dalla normativa vigente.

5. Nelle scuole gli impianti possono essere attivati esclusivamente negli orari di chiusura degli edifici, fatte salve necessità di giustizia.

6. Il sistema di videosorveglianza comporterà esclusivamente il trattamento di dati personali rilevati mediante le riprese televisive e che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti, i veicoli e qualsiasi altro mezzo di trasporto terrestre, aereo o acquatico che transiteranno nell'area interessata.

7. In ogni caso, le modalità di trattamento e di conservazione dovranno rispettare quanto disposto dalla vigente normativa, ed in particolare i dati personali oggetto di trattamento dovranno 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.

CAPO II
SOGGETTI COINVOLTI NEL TRATTAMENTO

Art. 7
Titolare del trattamento.

1. Il Titolare del trattamento dei dati personali acquisiti mediante gli impianti di cui al presente regolamento è il Comune di Mandello del Lario (LC). A tal fine il Titolare è rappresentato dal Sindaco pro tempore, a cui compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza.
2. Il Sindaco, in qualità di rappresentante del Titolare del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti:
a) definisce le linee organizzative per l'applicazione della normativa di settore, confrontandosi direttamente con il R.P.D. o interpellandolo per le questioni di competenza di quest'ultimo;
b) dispone, attraverso il Designato, le eventuali procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato ai sensi degli artt. 33 e 34 del RGPD;
c) dispone, sentito il R.P.D. ed attraverso il Designato, quando necessario, la valutazione di impatto sulla protezione dei dati di cui all'art. 35 del RGPD ed eventualmente la consultazione preventiva al Garante per la protezione dei dati personali di cui all'art. 36 RGPD, oltre a qualsiasi altra consultazione ritenuta necessaria per il corretto trattamento dei dati, interagendo con l'autorità nei casi previsti dalla norma;
d) nomina i Designati - o Supervisori - del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di cui al presente Regolamento, impartendo istruzioni ed assegnando compiti e responsabilità;
e) detta le linee guida di carattere fisico, logico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti;
f) vigila sulla puntuale osservanza delle disposizioni impartite.

Art. 8
Designato (supervisore) e Autorizzato.

1. Il responsabile della Polizia Locale viene nominato dal Sindaco quale "**Designato** del Trattamento" dei dati personali rilevati; il designato viene domiciliato, in ragione delle funzioni svolte, in Mandello del Lario presso il comando di polizia locale.
2. Il designato deve rispettare pienamente quanto previsto dal presente regolamento in tema di trattamento dei dati personali, dalle leggi vigenti, ivi incluso il profilo della sicurezza e dalle disposizioni del presente regolamento.
3. Il designato procede al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.
4. Gli **autorizzati** al materiale trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente al presente regolamento ed alle eventuali ulteriori istruzioni del titolare o del designato.
5. Il Designato custodisce le parole chiave di sistema - non le password dei dipendenti - e dispone di appropriate credenziali di amministrazione e governo dei sistemi. Nel caso la centrale di controllo con i monitor fosse in locali appositi, custodirà sotto la sua responsabilità le chiavi per l'accesso agli stessi e le chiavi degli armadi per la conservazione dei supporti per le immagini, file sonori o altri dati registrati.

Art. 9
Nomina, compiti e funzioni del "Designato".

1. La nomina è effettuata con atto del Sindaco ed i cui compiti sono analiticamente specificati di seguito:
a) individuerà e nominerà con propri atti i soggetti "Autorizzati al Trattamento" dei dati personali rilevati, impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni regolamentari, RGPD, nonché all'art 18 del D.Lgs 51/2018. Detti soggetti saranno esclusivamente appartenenti alla Polizia Locale e saranno opportunamente istruiti e formati da parte del designato, con riferimento alla tutela del diritto alla riservatezza nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati;
b) provvede a rendere l'informativa agli interessati secondo quanto definito dalle norme vigenti e dal presente regolamento;
c) verifica e controlla che il trattamento dei dati effettuato mediante i sistemi di videosorveglianza o geolocalizzazione siano realizzati nel rispetto dei principi di cui all'art. 5 del RGPD nonché all'art 3 del D. Lgs 51/2018 e, in particolare, assicura che i dati personali siano trattati in modo lecito, corretto e trasparente;

garantisce altresì che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;
d) assicura che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
e) tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e, in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, adotta tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del RGPD; nonché dell'art. 25 del D.Lgs 51/2018
f) consentire di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del RGPD;
g) assiste il Titolare nel garantire il rispetto degli obblighi di sicurezza, mettendo in atto misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti dell'Ente;
h) garantisce l'adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti dell'Ente;
i) assicura l'adozione di procedure volte a testare, verificare e valutare costantemente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento;
j) assiste il Titolare nelle eventuali procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato ai sensi degli artt. 33 e 34 del RGPD;
k) assiste il Titolare nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD e nella successiva eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità alla previsione di cui all'art. 36 del RGPD;
l) affianca il Titolare, in conformità alle disposizioni di cui all'art. 30, paragrafo 1, del RGPD, nell'istituzione e aggiornamento del Registro delle attività di trattamento, tenuto in forma scritta, anche in formato elettronico;
m) garantisce che il **Responsabile della Protezione dei Dati** designato dal Titolare del trattamento, sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e si impegna ad assicurargli l'affiancamento necessario per l'esecuzione dei suoi compiti;
n) mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa e per consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto incaricato;
o) è responsabile della custodia e del controllo dei dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta
p) assicura che i soggetti autorizzati si attengano, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantisce che vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali;
q) garantisce la tempestiva emanazione, sia verbalmente che per iscritto, di direttive ed ordini di servizio rivolti al personale autorizzato con riferimento ai trattamenti realizzati mediante gli impianti oggetto del presente regolamento, previo consulto del **Responsabile della Protezione dei dati**, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;
r) vigila sul rispetto da parte dei soggetti autorizzati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.

Art 10
Nomina, compiti e funzioni degli "Autorizzati".

1. Il Designato del trattamento autorizza i soggetti al trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di cui al presente Regolamento. L'autorizzazione è formalizzata con atto scritto, nel quale si rinvia al rispetto dei compiti affidati ai soggetti autorizzati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati, come previsto dal presente regolamento. I soggetti autorizzati sono scelti esclusivamente tra i componenti della polizia locale del comune di Mandello del Lario, tenendo conto della loro esperienza, capacità e affidabilità al fine di garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.
2. In particolare, i soggetti autorizzati devono:
a) utilizzare sempre solo le proprie credenziali personali per l'accesso ai sistemi informatici, garantendone la riservatezza; i sistemi devono garantire la registrazione degli accessi ed il tracciamento;

b) mettere in sicurezza gli strumenti di accesso alle informazioni e gli eventuali supporti di memorizzazione assegnati, in modo da evitare che i dati trattati siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
c) mantenere la massima riservatezza sulle informazioni di cui vengano a conoscenza nell'esercizio delle loro mansioni;
d) custodire e controllare e conservare i dati personali rispettando le misure di sicurezza predisposte dall'Ente, affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
e) evitare di creare banche dati nuove senza autorizzazione espressa del Designato al trattamento;
f) segnalare al Designato situazioni per cui, nello svolgimento delle attività assegnate, dovessero venire a conoscenza di informazioni eccedenti la propria autorizzazione al trattamento, oppure dovessero ravvisare elementi che potrebbero inficiare la sicurezza dei sistemi, dei dati trattati o dei supporti di memorizzazione;
g) fornire al Designato dei dati trattati ed al Responsabile della Protezione dei Dati, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo;
h) garantire la massima collaborazione in caso di istanze avanzate da parte degli interessati, di accertamenti/ispezioni da parte dell'Autorità Garante per la protezione dei dati personali e di richieste di accesso ai dati da parte di autorità giudiziarie o di polizia giudiziaria, attenendosi alle disposizioni del Designato o del Titolare.
3. I soggetti autorizzati, a cui viene impartita apposita formazione, devono trattare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del Designato.
4. La gestione e l'utilizzo dei sistemi di videosorveglianza aventi per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali è riservata agli organi di Polizia Locale, aventi qualifica di Ufficiali e/o Agenti di Polizia Giudiziaria.
5. L'utilizzo dei dispositivi di acquisizione da parte dei soggetti autorizzati al trattamento dovrà essere conforme ai limiti indicati dal presente Regolamento come eventualmente modificato ed integrato nonché alle specifiche istruzioni impartite.
6. In caso di sostituzione del Designato, persiste la validità delle autorizzazioni precedentemente attribuite, salvo che il nuovo Designato disponga diversamente; il nuovo Designato è comunque tenuto a verificare la sussistenza delle autorizzazioni precedentemente rilasciate, provvedendo al loro aggiornamento in caso di necessità.

Art. 11
Persone autorizzate ad accedere fisicamente ai sistemi e ai luoghi.

1. L'accesso ai locali ove sono presenti monitor o altri sistemi di ricezione dei dati raccolti è consentito solamente al personale in servizio presso la sede del comando di Polizia Locale di Mandello del Lario.
2. Eventuali accessi di persone diverse da quelli innanzi indicate devono essere autorizzati, per iscritto, dal Designato.
3. Possono essere autorizzati all'accesso solo incaricati di servizi rientranti nei compiti istituzionali dell'ente di appartenenza e per scopi connessi alle finalità di cui al presente regolamento, nonché il personale addetto alla manutenzione degli impianti ed alla pulizia dei locali e il personale delle Forze di Polizia.
4. Il Designato è responsabile della gestione e del trattamento, 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 avvalendosi del personale autorizzato.
5. Gli autorizzati di cui al presente regolamento vigilano sul puntuale rispetto delle istruzioni fornite dal Designato e sulla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.
6. Nel caso la centrale di raccolta dei dati fosse ubicata in locali specificatamente dedicati allo scopo, siano essi interni al comando, presso il municipio o in altri locali a ciò appositamente destinati, l'accesso è consentito esclusivamente al Titolare, al Designato, ai soggetti autorizzati e ad eventuali soggetti di cui al comma 3. L'accesso da parte di soggetti diversi da quelli precedentemente indicati è subordinato al rilascio, da parte del Titolare o del Designato, di un'autorizzazione scritta, motivata e corredata da specifiche indicazioni in ordine ai tempi ed alle modalità dell'accesso. L'accesso avviene in presenza di soggetti autorizzati dal Designato. L'accesso ai locali può essere consentito esclusivamente ad incaricati di servizi rientranti nei compiti istituzionali dell'ente di appartenenza e per scopi connessi alle finalità definite per lo specifico trattamento di dati, nonché al personale addetto alla manutenzione degli impianti ed alla pulizia dei locali.
7. In caso i dati personali siano custoditi in siti esterni a seguito di specifica prestazione di servizio conferita ad un responsabile esterno, quest'ultimo è tenuto a garantire l'adozione di adeguate misure di sicurezza fisica

al fine di ridurre al minimo il rischio di accesso non autorizzato ai sistemi e ai luoghi presso cui viene effettuato il trattamento.

Art. 12
Soggetti esterni che trattano dati per conto del Titolare.

1. Il Titolare del trattamento, anche tramite il Designato, ha la facoltà di avvalersi di soggetti esterni, in qualità di responsabili, per lo svolgimento di attività correlate alla gestione e al funzionamento dei sistemi, che potrebbero comportare, seppur in maniera accidentale, un trattamento di dati.
2. Queste attività possono comprendere la manutenzione tecnica degli impianti, l'amministrazione dei sistemi informatici, il backup delle informazioni, la profilazione delle utenze che accedono ai dati, la conservazione presso proprie infrastrutture tecnologiche dei dati acquisiti e tutte le operazioni che potrebbero comportare, per loro natura, delle criticità in merito alla protezione dei dati personali.
3. I soggetti a cui il Titolare ricorre in qualità di responsabili devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate che assicurino la tutela dei diritti dell'interessato.
4. Il Titolare disciplina i trattamenti effettuati da parte del responsabile mediante contratto ovvero altro atto giuridico, specificando obblighi e responsabilità ai sensi degli artt. 28 e 29, RGPD. La regolamentazione di tali impegni può essere formalizzata dal Titolare o dal Designato.
5. Il Designato tiene una lista dei responsabili esterni del trattamento.
6. I Designati, nell'ambito delle rispettive attività di gestione dei sistemi di videosorveglianza e coordinamento dei processi organizzativi, possono avvalersi dell'operato di soggetti autorizzati e di responsabili esterni attribuendo ad essi specifici ruoli, mansioni e responsabilità, fra cui:
a) accesso ai sistemi per la visualizzazione dei dati in tempo reale;
b) accesso ai sistemi per la consultazione dei dati registrati;
c) estrazione di copia dei dati in formato analogico e/o digitale e conversione in altri formati;
d) assegnazione di strumenti elettronici idonei per la consultazione dei dati;
e) attribuzione di specifici profili di accesso agli operatori;
f) riversamento di immagini e videoriprese acquisite tramite supporti di memorizzazione installati su dispositivi di acquisizione;
g) estrazione dei percorsi effettuati dagli strumenti di geolocalizzazione, eventualmente in forma anonima;
h) utilizzo di funzionalità avanzate dei dispositivi in dotazione (es. zoom, brandeggio, ecc);
i) assegnazione di compiti manutentivi;
j) attribuzione di mansioni di configurazione di sistemi e/o rilascio di credenziali con relativi profili di accesso;
k) assegnazione di qualsiasi altro incarico necessario per il corretto trattamento dei dati.
7. Ogni specifica attribuzione di ruoli e responsabilità deve essere formalizzata e accompagnata da apposite istruzioni organizzative ed operative.
8. L'attribuzione di profili di accesso, di strumenti operativi nonché di funzioni correlate al trattamento di dati deve essere effettuata a seguito di valutazione dell'esperienza, capacità e affidabilità dei soggetti destinatari, e previa adeguata formazione, al fine di garantire l'adeguata sicurezza dei sistemi e dei dati.

Art.13
Amministratori di Sistema. Responsabili esterni del trattamento - gestione tecnica degli impianti di videosorveglianza.

1. Tra le mansioni assegnate ai soggetti autorizzati o ai responsabili esterni possono rientrare attività tecniche di gestione e manutenzione di sistemi elaborativi o di loro componenti.
2. La gestione tecnica dell'impianto e le attività di manutenzione possono essere affidate a società esterne al Comune, appositamente nominate "Responsabile Esterno del trattamento" (art. 28 GDPR) d'ora in avanti denominata semplicemente Responsabile della Gestione Tecnica degli impianti di videosorveglianza.
3. Il Responsabile della gestione tecnica degli impianti di videosorveglianza dovrà:
a) curare l'installazione, la gestione e la manutenzione degli impianti di videosorveglianza;
b) assegnare le credenziali di accesso necessarie per l'utilizzo degli impianti di videosorveglianza.
4. Nella nomina di cui al precedente comma 2 saranno specificati i compiti, le responsabilità e le mansioni di amministrazione dei sistemi assegnati.
5. Coloro che svolgono mansioni di amministrazione dei sistemi informatici devono essere espressamente designati da soggetti aventi titolo di rappresentare il Titolare negli specifici contesti del trattamento.
6. Il Designato redige e mantiene aggiornato l'elenco degli amministratori di sistema designati fra il personale dell'Ente, oltre che l'elenco dei responsabili esterni che svolgono mansioni di amministrazione dei sistemi.
7. Questi ultimi, a loro volta, sono tenuti a mantenere aggiornato l'elenco delle persone fisiche che operano come amministratori di sistema per conto del Titolare, che dovrà essere reso disponibile su richiesta dell'Ente.

8. Il Designato e i responsabili sono tenuti, per i contesti di loro competenza e responsabilità, al rispetto delle prescrizioni specificate nel provvedimento del Garante Privacy sugli amministratori di sistema e aggiornamenti successivi.

Art. 14

Soggetti autorizzati al trattamento e dei preposti alla gestione dell'impianto di videosorveglianza.

1. I soggetti autorizzati devono:

a) per l'accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali di accesso personali, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;

b) conservare i supporti informatici contenenti dati personali in modo da evitare che detti supporti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;

c) mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali;

d) custodire e controllare i dati personali affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;

e) evitare di creare banche dati nuove senza autorizzazione espressa del designato del trattamento dei dati;

f) mantenere assoluto riserbo sui dati personali di cui vengano a conoscenza in occasione dell'esercizio delle proprie mansioni;

g) conservare i dati rispettando le misure di sicurezza predisposte dall'Ente;

h) fornire al Titolare dei dati trattati, al Designato ed al **Responsabile della Protezione dei dati**, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

2. I soggetti autorizzati devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alla istruzione del Titolare o del designato.

3. L'utilizzo degli apparecchi di ripresa da parte dei soggetti autorizzati al trattamento dovrà essere conforme ai limiti indicati dal presente Regolamento come eventualmente modificato ed integrato.

4. eventuali soggetti che svolgono, fra il personale dell'ente, mansioni di *amministratore di sistema* verranno appositamente designati dal Titolare del trattamento;

5. Nell'ambito dei designati/autorizzati, verranno individuati, con l'atto di nomina, i soggetti cui è affidata la custodia e conservazione delle chiavi di accesso alla sala operativa ed agli armadi per la conservazione dei supporti contenenti le immagini laddove esistano.

CAPO III
TRATTAMENTO DEI DATI PERSONALI

Art. 15
Diretta visione delle immagini - acquisizione dati.

1. La diretta visualizzazione delle immagini rilevate con i sistemi di videosorveglianza o geolocalizzazione nella centrale operativa è limitata ad obiettivi particolarmente sensibili e strategici per la sicurezza urbana o in presenza del requisito di pubblico interesse (necessità, pertinenza, non eccedenza dei dati o dei trattamenti). Le immagini dirette devono essere viste solo dagli appartenenti alla Polizia Locale o delle Forze di Polizia autorizzate.
2. Il designato o gli autorizzati si obbligano a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto.
3. Il flusso dei dati può giungere anche direttamente agli operatori di Polizia Locale, in grado di garantire i servizi di monitoraggio sul posto ed il conseguente, eventuale, intervento immediato utilizzando supporti che permettano la sola visualizzazione degli elementi utili e necessari alla contestazione immediata di violazioni al C.d.S. e/o ad interventi finalizzati a reprimere reati o violazioni amministrative per cui è possibile impiegare videoriprese o geolocalizzazione.
4. I dati sono acquisiti tramite strumenti idonei al perseguimento delle finalità del Titolare, attraverso memorizzazione su specifici supporti installati sulle periferiche di acquisizione o trasmissione verso una centrale di acquisizione dei dati.

Art. 16
Modalità di raccolta e requisiti dei dati personali – Scelta e luoghi d'installazione apparati - Tempi di conservazione.

1. L'installazione delle telecamere avviene esclusivamente nei luoghi pubblici (strade, piazze, immobili, parchi o aree verdi), o in altre aree su cui è stata concessa l'installazione o in presenza di accordi tra le parti.
2. I sistemi di acquisizione di immagini, geolocalizzazione o telecamere modulari - fototrappole - sono installati in risposta ad esigenze rappresentate dal Sindaco o dalla Giunta Comunale al Designato. Le esigenze dovranno essere motivate da un'appropriata analisi di contesto nel rispetto del principio di proporzionalità.
3. Spetta esclusivamente al Designato definire il numero, la tipologia ed il luogo ove porre gli apparati di ripresa, geolocalizzazione, telecamere modulari e quant'altro sia ritenuto necessario ed opportuno per raggiungere e dare risposta alle esigenze espresse dal Sindaco o dalla Giunta Comunale. Questo in conformità con la propria autonomia organizzativa che esclude, quindi, la possibilità che altri Servizi o Strutture comunali possano installare, attivare o chiedere di collegare impianti diversi da quelli individuati con le procedure sopra descritte. Ciò che verrà installato senza rispettare le procedure sopra indicate non verrà collegato al sistema gestito dalla polizia locale e ne risponderà chi ha disposto la realizzazione dell'impianto.
4. Le modalità di acquisizione, trattamento e conservazione dati dovranno rispettare quanto disposto dalla vigente normativa, ed in particolare i dati personali oggetto di trattamento dovranno 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.
5. L'utilizzo del brandeggio o dello zoom, qualora possibile, da parte dei soggetti autorizzati avviene nel rispetto dei limiti previsti dal presente regolamento.
6. L'attività di videosorveglianza o geolocalizzazione deve raccogliere solo dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando solo immagini e dati indispensabili, limitando l'angolo di visuale delle riprese, evitando (quando non strettamente indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti.
7. Il designato e gli autorizzati al trattamento dei dati personali si obbligano a non effettuare riprese di dettaglio dei tratti somatici delle persone fisiche che non siano funzionali alle finalità istituzionali dell'impianto attivato. I segnali video delle unità di ripresa sono inviati presso la sede del comando di Polizia Locale o datacenter individuato appositamente dove sono registrati su appositi server. I video possono essere visionati dalle Forze di Polizia solo se debitamente autorizzate. L'impiego del sistema di videoregistrazione è necessario per ricostruire l'evento, ai fini del soddisfacimento delle finalità di consentite dalle norme e dal presente regolamento.
8. I dati personali oggetto di trattamento sono:
a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per le finalità di cui all'art. 3 del presente Regolamento e resi utilizzabili in altre operazioni di trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi;

c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati.

9. La **conservazione dei dati**, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza per la finalità di sicurezza urbana limitata al **massimo 7 giorni**, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Per tutte le altre finalità, così come individuate nell'art. 3, si ritiene congruo un periodo di conservazione di 4 giorni. Per i dispositivi mobili quali bodycam, dash cam, droni, videocamere ricollocabili e telefonia mobile la conservazione è fissata in 3 giorni. I periodi di conservazione sin qui individuati possono essere diversi quando necessari e riferiti a finalità che trovano riferimenti normativi specifici.

10. Nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza pubblica, alla luce delle richiamate disposizioni normative, il termine massimo di durata della conservazione e definito a seconda dello scenario concreto, fatte salve specifiche esigenze di ulteriore conservazione.

11. In ragione di necessità investigative e su richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria il Responsabile potrà disporre la conservazione delle immagini per un periodo di tempo superiore ai sette giorni.

12. Il sistema di videoregistrazione impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

13. In caso di cessazione del trattamento, i dati personali sono distrutti.

14. Le immagini riprese dalle telecamere dovranno venire memorizzate in formato elettronico su un unico (o un numero limitato) supporto di memorizzazione di massa centralizzato e ben individuato all'interno di un unico e ben determinato apparato di tipo "server" (può essere comunque fatta salva la necessità di una memorizzazione "di backup" anche su un server remoto). Il suddetto server dovrà essere dedicato esclusivamente alla memorizzazione delle immagini registrate dalle telecamere del sistema di videosorveglianza, e non dovrà essere dedicato ad altri scopi. Se non diversamente disposto dal titolare con atto scritto, il server non dovrà essere collegato ad internet, oppure dovrà essere collegato solo in casi e per finalità specifiche e ben individuate, per intervalli di tempo il più possibile contenuti e con le dovute protezioni allo stato dell'arte.

15. Non è consentita la memorizzazione "ordinaria" delle immagini in locale a livello di postazione "client", o comunque su supporti e strumenti diversi dal succitato server centralizzato. La memorizzazione temporanea delle immagini è consentita solamente in aree appositamente dedicate del server, nel qual caso la copia temporanea delle immagini estratte dovrà essere cancellata non appena possibile.

16. Non si dovranno rispettare i dettati dei commi 14 e 15 sino all'adozione delle modifiche necessarie agli impianti in seguito ad intervenute mutate disposizioni normative o innovazioni tecnologiche che rendessero inadeguato quanto previsto.

Art. 17
Modalità da adottare per i dati video ripresi. Accesso ai sistemi ed alle immagini.

1. I monitor degli impianti di videosorveglianza sono collocati in modo tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate.

2. L'accesso ai sistemi che gestiscono i dati oggetto del presente Regolamento e ai dati oggetto dello specifico trattamento può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide e strettamente personali, rilasciate su disposizione del Designato al trattamento.

3. L'accesso ai dati registrati al fine del loro riesame, nel rigoroso arco temporale previsto per la conservazione, è consentito solamente in caso di effettiva necessità per il perseguimento delle finalità definite per lo specifico trattamento di dati.

4. L'accesso alle immagini da parte del designato e degli autorizzati del trattamento dei dati si limita alle attività oggetto della sorveglianza; eventuali altre informazioni di cui vengano a conoscenza mentre osservano il comportamento di un soggetto ripreso, non devono essere prese in considerazione. Gli strumenti assegnati che consentano l'accesso ai dati devono essere protetti da sistemi di autenticazione e non devono essere lasciati incustoditi.

5. Nel caso le immagini siano conservate, i relativi supporti che dovranno essere crittografati, vengono custoditi per l'intera durata della conservazione in un armadio o simile struttura dotato di serratura, apribile solo dal designato e dagli autorizzati del trattamento dei dati. I soggetti autorizzati sono tenuti a garantire la custodia in sicurezza degli strumenti utilizzati e dei supporti di memorizzazione impiegati, prestando la massima attenzione durante il loro impiego e riponendoli nei luoghi destinati alla loro conservazione, in modo da ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati. Qualora la presa in carico delle immagini e delle videoriprese venga effettuata tramite riversamento dai supporti di

memoria presenti negli strumenti di acquisizione, i file contenenti dati devono essere rimossi dai supporti una volta acquisiti i dati.
6. La cancellazione delle immagini sarà garantita mediante gli strumenti e le procedure tecnologiche più avanzate; le operazioni di cancellazione devono essere effettuate esclusivamente all'interno dell'ambiente a ciò deputato sito all'interno del comando di Polizia Locale.
7. Nel caso il supporto debba essere sostituito per eccessiva usura, sarà distrutto in modo da renderlo inutilizzabile, non permettendo il recupero dei dati in esso presenti.
8. L'accesso alle immagini ed ai dati personali è consentito:
a) al Titolare, al Designato ed ai soggetti autorizzati al trattamento;
b) alle Forze di Polizia (sulla base di richiesta scritta formulata dal rispettivo comando di appartenenza e acquisita dall'Ente) nonché per finalità di indagine dell'Autorità Giudiziaria (sulla base di formale richiesta proveniente dal Pubblico Ministero e acquisita dall'Ente);
c) ai responsabili incaricati della manutenzione dei sistemi (Responsabili della Gestione Tecnica di cui all'art. 13 del presente regholamento) nei limiti strettamente necessari alle specifiche esigenze di funzionamento dell'impianto medesimo ovvero, in casi del tutto eccezionali, agli amministratori di sistema dell'ente specificamente designati per tale contesto (preventivamente autorizzati al trattamento dei dati);
d) all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso, previo accoglimento della relativa richiesta. L'accesso da parte dell'interessato sarà limitato ai soli dati che lo riguardano direttamente; al fine di evitare l'accesso ad informazioni riguardanti altri soggetti, dovranno pertanto essere utilizzati, da parte dell'Ente, adeguati accorgimenti tecnici in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti;
e) ai soggetti legittimati all'accesso ai sensi e per gli effetti degli artt. 22 e ss. L. 241/90 e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'art. 24, comma 7, L. 241/90, l'accesso ai dati sia necessario per curare o per difendere gli interessi giuridici del richiedente. L'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante;
f) agli altri Enti-Soggetti Pubblici e/o Organi di sicurezza pubblica (Autorità di Protezione Civile, VV.FF. Autorità sanitarie, Province o Regioni, ect.), previa richiesta scritta motivata o accordo scritto, ed agli altri casi specificamente previsti dal presente Regolamento.
9. Tutti gli accessi alla visione saranno documentati e registrati tramite sistema automatico di log.
10. Non possono essere rilasciate copie delle immagini registrate concernenti soggetti diversi dall'interessato, salvi i casi particolarmente meritevoli di tutela.

Art. 18
Comunicazione - Sicurezza nelle trasmissioni.

1. La comunicazione dei dati personali da parte dell'Ente a favore di soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da una norma di legge o regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria ed esclusivamente per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'art. 2 ter del D.Lgs. n. 196/03.
2. È in ogni caso fatta salva la comunicazione o diffusione di dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'art. 58, comma 2, del D. Lgs. 30/6/2003, n. 196 per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.
3. La trasmissione attraverso reti pubbliche di comunicazioni di immagini, video e/o audio-riprese e dati di geolocalizzazione acquisite tramite dispositivi sarà effettuata previa applicazione di tecniche di cifratura che ne garantiscano la riservatezza.
4. Sarà possibile diffondere dati raccolti dai sistemi di sorveglianza attraverso social, testate giornalistiche TV e radio d'informazione generale solo se finalizzati a raggiungere scopi d'interesse sociale rilevante quali campagne di sensibilizzazione su temi quali l'abbandono rifiuti, abbandono animali, danneggiamenti e/o cura delle proprietà pubbliche o private, comportamenti scorretti nella circolazione stradale o sulle acque, etc. Il tutto adottando misure per tutelare la riservatezza sui coinvolti e dei soggetti estranei.
5. I Designati sono tenuti a disporre l'adozione di adeguati sistemi di sicurezza per garantire la riservatezza delle trasmissioni telematiche nei contesti di propria competenza e responsabilità.

Art. 19
Limiti alla utilizzabilità di dati personali.

1. I dati personali trattati in violazione della disciplina in materia di trattamento dei dati personali non possono essere utilizzati ai sensi dell'art. 2 decies del D. Lgs. n. 196/03, salvo quanto previsto dall'art. 160 bis dello stesso decreto.

Art. 20
Tipi di trattamenti autorizzati – video e vocali.

1. Nell'installazione e nell'esercizio del sistema di videosorveglianza, sono autorizzati esclusivamente le seguenti tipologie di trattamenti:

a) installazione e attivazione di nuove telecamere;
b) creazione e gestione di gruppi e profili di utenti;
c) consultazione immagini live da telecamera;
d) messa a fuoco, brandeggiamento e zoom delle telecamere;
e) impostazione di limiti al brandeggiamento delle telecamere;
f) impostazione di zone oscurate staticamente anche al fine di non riprendere elementi estranei alle necessità di trattamento;
g) registrazione di immagini;
h) cancellazione di immagini;
i) predisposizione delle soglie temporali e degli eventi di cancellazione immagini;
j) consultazione immagini registrate;
k) estrazione (duplicazione) immagini registrate;
l) definizione aree di motion-detection;
m) definizione azioni da eseguire in concomitanza di eventi di motion-detection;
n) accensione di sorgenti luminose o ad infrarosso;
o) rilevazione e inventario degli indirizzi IP presenti in rete;
p) rilevazione e inventario dei mac address presenti in rete;
q) installazione e configurazione di software applicativo;
r) installazione e configurazione di software di base;
s) installazione di "patch" e "hot fix";
t) attivazione collegamenti da remoto;
u) interventi generici di manutenzione e configurazione hardware e software
v) attivazione e configurazione di meccanismi di tracciatura ("logging");
w) estrazione e conservazione di files di log;
x) apposizione di forma digitale qualificata e di marcatura temporale e files di log;
y) apposizione di forma digitale qualificata e marcatura temporale ad immagini e sequenze filmiche.

2. Nell'installazione e nell'esercizio di sistemi di registrazione audio presso il comando di P.L. con apparati telefonici o mediante apparati mobili in dotazione al personale, sono autorizzati esclusivamente le seguenti tipologie di trattamenti:

a) registrazione di tutte le telefonate in ingresso e uscita dagli appartai fissi presenti in comando;
b) registrazione di tutte le telefonate in ingresso e uscita dagli apparati mobili in dotazione al personale di P.L.;
c) tempo di conservazione massimo delle registrazioni vocali: 7 giorni con cancellazione automatica;
d) registrazione di audio/video anche attraverso dispositivi di proprietà degli operatori di P.L. solo per finalità connesse alla rilevazione di violazioni amministrative e/o penali e per eventi in cui possa ritenersi opportuno raccogliere elementi su quanto accade in presenza dell'operatore per la prosecuzione dell'attività istituzionale.
e) tempo di conservazione massimo delle registrazioni avvenute con dispositivi privati: 3 giorni, con cancellazione anche manuale. I dati raccolti dovranno essere salvati su supporti informatici di proprietà del comando di P.L. per la prosecuzione delle attività istituzionali e comunque conservati per un massimo di 7 giorni. Il tutto salvo necessità legate a procedimenti penali o amministrativi in cui sia necessario conservare oltre i dati raccolti.

CAPO IV
DIRITTI DEGLI INTERESSATI

Art. 21
Informativa.

1.Gli interessati devono essere sempre informati del trattamento effettuato dal Titolare.
2.L'Ente, in ottemperanza a quanto disposto dall'art. 13 del Reg. UE n. 679/16 (G.D.P.R.) e del D. Lgs. n. 51/2018, si obbliga ad affiggere un'adeguata segnaletica permanente, nelle strade, nelle piazze ed in ogni altra area in cui sono posizionate telecamere.
3. I soggetti interessati che stanno per accedere o che si trovano in una zona videosorvegliata devono essere informati mediante appositi cartelli conformi ai modelli approvati dall'Autorità Garante per la protezione dei dati personali. L'informazione deve essere fornita anche nei casi di eventi e in occasione di spettacoli pubblici se l'area in cui stanno per accedere è sottoposta a videosorveglianza.
4. In presenza di più telecamere, o in relazione all'area e alle modalità delle riprese, sono installati più cartelli.
5. Per l'informazione si utilizzerà un'nformativa cosiddetta di "primo" e di "secondo livello".
6. Quanto all'informativa di "**primo livello**", finalizzata per relazionarsi in modo primario e diretto con l'interessato, il Titolare utilizzerà un cartello di avvertimento per dare una visione di insieme del trattamento previsto in modo facilmente visibile, comprensibile e chiaramente leggibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno. Il cartello dovrà essere posizionato prima di entrare nell'area di riresa dell'impianto, all'interno dell'area monitorata o sotto l'impianto stesso quando non vi sono possibilità per rispettare altre posizioni. Detto cartello riporterà le informazioni più importanti, comprese quelle di maggior impatto per l'interessato (ad esempio: finalità del trattamento, identità del Titolare, i dati di contatto del Responsabile della Protezione dei Dati e i diritti degli interessati, il periodo di conservazione, le modalità di trasmissione). Verrà inoltre riportato anche il luogo ove l'interessato potrà prendere visione dell'informativa per esteso e/o l'eventuale possibilità di prendere visione dell'informativa mediante "bar-code", "QR code" o similari.
7. In presenza di più dispositivi di acquisizione, in relazione alla vastità dell'area e alle modalità delle riprese, potranno essere installati più cartelli informativi.
8. Quanto all'informativa di "**secondo livello**", essa verrà resa disponibile in luogo facilmente accessibile all'interessato come, ad esempio, il sito istituzionale dell'Ente, e dovrà contenere tutte le informazioni obbligatorie previste dall'art. 13 RGPD. Sul sito istituzionale del Comune è pubblicata l'informativa completa contenente le modalità e le finalità degli impianti di videosorveglianza, la modalità di raccolta e conservazione dei dati e le modalità di diritto di accesso dell'interessato secondo quanto previsto dal Regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, e al D. Lgs. n. 51/2018, relativo 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. Inoltre sarà resa disponibile l'indicazione dell'esatta collocazione di tutti gli impianti fissi di acquisizione immagini, anche attraverso geo localizzazione.
9. L'Ente, nella persona del designato, si obbliga ad informare preventivamente la comunità cittadina dell'avvio del trattamento dei dati personali effettuato tramite l'impianto di videosorveglianza, anche attraverso una sua mappatura, dell'eventuale incremento dimensionale dell'impianto stesso e dell'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale, tra cui il portale istituzionale.
10. L'informativa di cui sopra non è dovuta nel caso di utilizzo di telecamere a scopo investigativo a tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati o violazioni amministrative non diversamente perseguibili.
11. Nel caso in cui il trattamento preveda la sorveglianza di una zona di ampia dimensione, si provvederà ad informare i soggetti interessati, tramite apposita diffusione sul sito istituzionale, dell'individuazione della zona soggetta al trattamento.
12. In caso di acquisizione di dati di geolocalizzazione, il Titolare dovrà fornire agli interessati un'informativa comprensiva di tutti gli elementi contenuti nell'art 13 del RGPD e dovrà apporre sui dispositivi e sui veicoli oggetto di geolocalizzazione un'adeguata informativa semplificata di facile comprensione.
13. Le registrazioni di telefonate comportano l'informativa solo con specifico richiamo nel sito istituzionale dell'Ente.

Art. 22
Diritti dell'interessato.

1. In relazione al trattamento dei dati personali l'interessato, in seguito a presentazione di apposita istanza scritta, ha diritto:

a) di conoscere l'esistenza di trattamenti di dati che possono riguardarlo, di ottenere conferma dell'esistenza o meno di dati personali che lo riguardano e la trasmissione in forma intellegibile dei medesimi e della loro origine;

b) di essere informato sugli estremi identificativi del titolare e del designato al trattamento, oltre che sulle finalità e le modalità del trattamento dei dati;

c) di ottenere dal Designato la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi nelle modalità previste dal presente Regolamento;

d) ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali e di tutto quanto previsto ex art. 13 del RGPD;

e) di richiedere la cancellazione nei casi previsti dal RGPD qualora sussista uno dei motivi di cui all'art. 17 del RGPD, nonché la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

f) di opporsi, nei casi previsti dal RGPD, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21 del RGPD. Il designato informerà l'interessato sull'esistenza o meno di motivi legittimi prevalenti;

g) di ottenere dal designato la limitazione del trattamento quando ricorre una delle ipotesi specificate all'art. 18 del RGPD. In tali casi i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

2. 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 o per ragioni familiari meritevoli di protezione.

3. Nell'esercizio dei propri diritti l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può altresì farsi assistere da persona di fiducia.

4. 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.

5. Per ciascuna delle richieste di cui al comma 1, può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati e comprensivi dei costi del personale, secondo quanto stabilito con apposito atto dell'Ente nel rispetto delle modalità previste dalla normativa vigente.

6. Le istanze di cui al presente articolo possono essere trasmesse al titolare o al designato mediante piattaforma presente sul sito istituzionale del comune, lettera raccomandata e posta elettronica. L'istanza per l'esercizio dei diritti dell'interessato è presentata al Responsabile della Protezione dei Dati dell'Ente, ai sensi dell'art. 38, paragrafo 4 del RGPD ovvero al designato dal Titolare, che, laddove necessario, si consulterà con il Responsabile della Protezione dei Dati.

7. Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

CAPO V
MISURE DI SICUREZZA.

Art. 23
Criteri e modalità di estrazione delle immagini richieste.

1. L'estrazione di immagini o di intere riprese, mediante duplicazione, potrà avvenire solo in presenza di autorizzazione da parte del Titolare del trattamento o del Designato, rilasciata a fronte di richiesta scritta e motivata.
2. Alle registrazioni delle immagini video il sistema deve apporre elementi che rispondano all'esigenza della necessaria garanzia dell'originalità della copia, seguendo lo stato dell'arte delle tecnologie in corso.
3. All'atto della consegna al soggetto richiedente del supporto di memorizzazione contenente le immagini estratte l'operatore, o comunque chi materialmente consegnerà il suddetto supporto di memorizzazione, dovrà far firmare e trattenere apposito documento che attesti la consegna e la ricevuta delle immagini estratte; detto documento dovrà fare riferimento alla richiesta originaria di estrazione.
4. Si dovrà inoltre compilare apposito **registro** dove si terrà traccia di giorno, data e ora di effettuazione dell'estrazione, del numero di protocollo della richiesta e della data di consegna.
5. Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare le informazioni utili alla sua identificazione tramite il sistema di videosorveglianza, fra cui il luogo, la data, l'intervallo temporale da estrarre e collocare su supporto esterno di memorizzazione di massa.
6. Il Designato accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della loro acquisizione, in ossequio alla previsione di cui all'art. 15, paragrafo 4 del RGPD.
7. Qualora il Designato non sia in grado di identificare l'interessato o in caso di richieste eccessive o manifestamente infondate da parte dell'interessato, il Designato – previa adeguata motivazione – informerà l'interessato dell'impossibilità di dare seguito alla richiesta.
8. In caso di richiesta di accesso ai dati di geolocalizzazione, l'interessato potrà chiedere di consultare tutti i dati in possesso del Titolare, fornendo tutte le informazioni necessarie per determinare specificamente i contesti che lo riguardano, come gli strumenti e i veicoli utilizzati oltre che il periodo di utilizzo.
9. Qualora, ai sensi dell'art. 15, paragrafo 3 del RGPD, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files i dati in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della loro acquisizione, in ossequio alla previsione di cui all'art. 15, paragrafo 4 del RGPD.

Art. 24
Ottemperanza al Provvedimento del 27-11-2008 del Garante per la protezione dei dati personali relativo al controllo dell'operato degli amministratori di sistema.

1. Per garantire l'ottemperanza a quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 27-11-2008 relativo al controllo dell'operato degli amministratori di sistema, il presente Regolamento prevede quanto segue:
a) a livello di software di videosorveglianza, deve essere attivato (ed eventualmente configurato) un meccanismo di "logging" (tracciatura) delle operazioni di amministrazione e gestione di sistema effettuate con profilo di "administrator";
b) a livello di software di videosorveglianza, il suddetto file di log non deve essere sovrascritto per un periodo minimo di 6 mesi;
c) il suddetto file di log non dovrà essere per nessun motivo cancellato, modificato o alterato durante il suddetto periodo;
2. La copia estratta del file di log dovrà essere generata in un formato non modificabile.

Art. 25
Requisiti minimi sul luogo di collocazione del server.

1. Il server di memorizzazione delle immagini dovrà essere fisicamente collocato all'interno di un locale che fornisca adeguate garanzie di sicurezza fisica e perimetrale. Di seguito si riportano i requisiti minimi che il locale dovrà soddisfare:
a) di norma chiuso a chiave, con serratura e chiave funzionante;
b) di norma assenza di materiale facilmente infiammabile in adiacenza del server;
c) presenza nelle vicinanze di almeno un estintore non a polvere, funzionante e regolarmente revisionato con frequenza almeno semestrale;

2. In aggiunta a quanto elencato al comma 1, è auspicabile (ancorché non strettamente obbligatoria) la presenza di quanto segue:
a) allarme volumetrico (attivato dalla variazione della volumetria all'interno dei locali) o di prossimità;
b) collegamento dei sensori e dell'allarme con centrale operativa di sicurezza, con le forze di Polizia dello Stato o con appartenenti alla Polizia Locale del comune di Mandello del Lario.

Art. 26
Requisiti minimi sugli strumenti elettronici, informatici e telematici.

1. Gli strumenti elettronici, informatici e telematici utilizzati nelle operazioni di trattamento dei dati, dovranno soddisfare i seguenti requisiti minimi:
a) sistema operativo server e client non obsoleto e con supporto attivo da parte del fornitore; non sono consentiti sistemi operativi obsoleti o poco sicuri e non aggiornati;
b) presenza di almeno due profili distinti: uno di tipo "administrator" e uno di tipo "utente normale", sia a livello di sistema operativo sia a livello di programma applicativo;
c) assegnazione e utilizzo delle user-id su base strettamente personale e non di gruppo;
d) possibilità di individuare e rimuovere periodicamente le vulnerabilità e le configurazioni poco sicure a livello applicativo e di sistema operativo;
e) protezione adeguata da virus e codici maligni;
f) protezione perimetrale adeguata in caso di apertura, anche temporanea, ad Internet.

Art. 27
Obblighi degli autorizzati.

1. L'utilizzo del brandeggio e dello zoom dovrà essere conforme ai limiti indicati nel presente regolamento e dalle norme in materia.
2. L'utilizzo delle telecamere è consentito solo per il controllo di quanto si svolge nei luoghi pubblici o aperti al pubblico, mentre esso non è ammesso verso le proprietà private.
3. Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione, solo in caso di effettiva necessità per il conseguimento delle finalità di cui agli artt. 3 e 6 e a seguito di regolare autorizzazione di volta in volta dal designato.
4. La mancata osservanza degli obblighi previsti al presente regolamento comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, di sanzioni amministrative oltre che l'avvio degli eventuali procedimenti penali.

Art. 28
Sicurezza dei dati.

1. I dati personali oggetto di trattamento sono custoditi ai sensi e per gli effetti dei precedenti articoli. Alle immagini, i supporti informatici ed i dati custoditi nel comando di Polizia Locale può accedere solo ed esclusivamente il personale in servizio nella Polizia Locale di Mandello del Lario debitamente istruito sull'utilizzo dell'impianto e debitamente incaricato ed autorizzato per iscritto dal Titolare del trattamento o Designato.
2. Il Designato alla gestione e al trattamento 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 designato al trattamento nomina gli autorizzati in numero sufficiente a garantire la gestione del servizio di videosorveglianza e dei sistemi di lettura targhe esclusivamente tra coloro che hanno qualifiche connesse allo svolgimento di funzioni di Polizia Locale nell'organico dei dipendenti del comune di Mandello del Lario .
4. Gli **autorizzati** andranno nominati esclusivamente tra gli operatori di P.L. in servizio che, per esperienza, capacità ed affidabilità, forniscono idonea garanzia nel rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.
5. La gestione degli impianti di videosorveglianza intesi in senso generale, degli apparati di registrazione audio, dei sistemi di lettura targhe e apparati per il rilevamento violazioni amministrative e/o penali è riservata agli operatori di Polizia Locale.

Art. 29
Cessazione del trattamento dei dati.

1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati personali sono:
a) distrutti in maniera tale da non poter essere, in nessun modo, recuperati;
b) conservati per fini esclusivamente istituzionali dell'impianto attivato, secondo quanto previsto dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e dall'art. 2 del D.Lgs. 51/2018 relativo 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.
c) ceduti ad altro Titolare purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti.
3. La cessazione dei dati in ogni caso è conforme alle disposizioni del RGPD.

Art. 30
Trasmissione dei video – audio.

1. Al fine di garantire la sicurezza della trasmissione dei dati, gli stessi dovranno essere comunicati adottando le opportune misure di sicurezza volte alla tutela del dato manipolato utilizzando tecniche e apparecchiature allo stato dell'arte esistenti al momento dell'esigenza.

CAPO VI
ACCESSO AI DATI DA PARTE DI ALTRI SOGGETTI.

Art. 31
Accordi con enti pubblici e privati.

1. È prevista la possibilità da parte del Titolare di stipulare accordi (convenzioni, protocolli di intesa, etc.) con soggetti pubblici e privati, al fine di consentire d'attivare ed effettuare la videosorveglianza, intesa nel senso più ampio del termine, con utilizzo di qualsiasi strumento tecnologico disponibile, di aree e territori che non siano di competenza o proprietà pubblica comunale (ad es. strade provinciali o statali, centri sportivi o palestre date in concessione a privati, aree private di uso pubblico, stazioni ferroviarie, porti, discariche rifiuti, aree montane o boschive, aree litoranee o adiacenti la lago, etc.).

Art. 32
Accesso ai dati da parte delle Forze di Polizia, Polizia Locale e dell'Autorità Giudiziaria.

1. La Direttiva 2016/680 del Parlamento europeo e del Consiglio d'Europa, 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, introduce la regolamentazione delle protezione delle persone fisiche con riferimento al trattamento dei dati da parte delle autorità a fini di prevenzione, investigazione e repressione di reati.
2. In base alla direttiva le Forze di Polizia o l'Autorità Giudiziaria possono lecitamente richiedere di:
a) accedere alle immagini "live", accedere alle immagini registrate ed ottenete copia delle registrazioni, effettuare riprese e registrazioni ad-hoc";
b) le richieste di accesso/estrazioni dovranno essere presentate per iscritto - o in forma orale per necessità urgenti ed inderogabili, cui farà seguito richiesta scritta - e seguire le procedure definite nel presente regolamento ed essere autorizzate dal Designato;
c) in ogni caso l'utilizzo delle immagini da parte di qualsiasi soggetto pubblico che, per l'esercizio delle proprie funzioni istituzionali, abbia necessità di accedere ai dati dovrà avvenire conformemente a quanto previsto dal Regolamento Europeo 2016/679 e dal D. Lgs. 196/2003 s.m.i. e più in generale dalla disciplina rilevante vigente in materia di privacy e sicurezza, con particolare riferimento al provvedimento generale del Garante per la protezione dei dati personali del 8 aprile 2010, dedicato alla videosorveglianza ed eventuali altre disposizioni successive.
3. Ove dovessero essere rilevate informazioni identificative di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica, della tutela ambientale e del patrimonio, il Designato che ha acquisito i dati o un soggetto debitamente autorizzato provvederà a darne immediata comunicazione agli organi competenti.
4. Solo gli organi delle Forze di Polizia, Polizia Locale e l'Autorità Giudiziaria potranno accedere alle informazioni raccolte, tramite consultazione presso la sede del Titolare, trasmissione telematica o consegna di copia su supporto digitale o analogico.

Art. 33
Accesso telematico da parte dell' Autorità Giudiziaria.

1. È previsto che l'Autorità Giudiziaria, previa stipula di una convenzione/accordo tra le parti deputate alle indagini possa accedere remotamente, in via telematica, ai sistemi di videosorveglianza in uso al comune di Mandello del Lario per accelerare i tempi di indagine e per sgravare il personale di Polizia Locale. Gli accessi dovranno avvenire su base nominativa individuale, e dovranno venire tracciati (log).

Art. 34
Accesso da parte di privati o loro delegati - altri servizi interni o Enti esterni.

1. E' consentita l'estrazione di copia dei dati acquisiti, nonché il riversamento su supporto digitale o analogico, ai fini della difesa di un diritto in riscontro ad un'istanza di accesso esclusivamente per indagini difensive in procedimenti giudiziari, per necessità connesse a ricorsi od opposizioni a violazioni amministrative e nei casi in cui le forze di polizia e polizie locali non siano intervenute per risalire a responsabilità in eventi che abbiano causato danni a persone e/o cose previa specifica e dettagliata richiesta motivata scritta.
2. Le attività di estrazione e riversamento dati di cui sopra possono essere svolte esclusivamente da soggetti appositamente autorizzati al trattamento.
3. I supporti digitali o analogici su cui vengono riversati i dati devono essere custoditi in sicurezza.
4. Al di fuori dei diritti dell'interessato e di quanto specificato nel presente Regolamento, l'accesso ai filmati della videosorveglianza è consentito con le sole modalità previste dalla normativa vigente. Possono essere

divulgate immagini provenienti da impianti di videosorveglianza solo previa anonimizzazione di ogni dato che consenta di identificare i soggetti ripresi

5. Ogni richiesta dovrà essere formulata per iscritto, motivata ed indirizzata al Designato entro e non oltre 7 giorni dall'evento.

6. Nel caso di incidenti stradali *senza l'intervento della polizia stradale* gli interessati (privati coinvolti e/o compagnie assicuratrici interessate) possono, entro 7 giorni dall'evento, presentare richiesta di "limitazione del trattamento" secondo quanto dispone l'art.12 paragrafo 1, lettere b) e c) della direttiva 95/46/CE in forza dell'art. 18 paragrafo 1 lettera c) del GDPR per ottenere la limitazione del trattamento - benché il comune non ne abbia più bisogno - ed al fine di fornire all'interessato i dati per l'accertamento, l'esercizio e la difesa di un diritto in sede civile o giudiziaria. Le immagini saranno consegnate su appositi supporti informatici solo previo pagamento anticipato delle relative spese individuate con apposita deliberazione di Giunta Comunale. Se i supporti informatici con le immagini richieste non saranno ritirate entro 7 giorni dalla comunicazione all'interessato della disponibilità saranno eliminate in forma permanente e non recuperabile.

7. Nell'eventualità che i filmati richiesti dall'interessato esistano, e immagini verranno fornite con estrazione delle sole parti d'interesse, oscurando o rendendo inutilizzabili immagini e dati riguardanti altri elementi estranei alle necessità del richiedente. In via generale, per quanto possibile, al fine di soddisfare le necessità del richiedente si forniranno informazioni attraverso comunicazione scritta delle risultanze degli accertamenti su ciò che è rilevabile dai sistemi di controllo e, sempre solo se compatibile con la tutela della riservatezza, potranno essere fornite stampe di singoli fotogrammi dell'evento interessato o brevissimi filmati (non più di 1 minuto) in cui verranno oscurate in maniera irrecuperabile le parti ed i dati non interessati dall'evento oggetto della richiesta

8. Nel caso di incidenti stradali *con l'intervento di forze di polizia stradale* i filmati saranno richiesti ed acquisiti dall'organo di polizia stradale che ha proceduto ai rilievi e in capo al quale è l'istruttoria relativa all'incidente.
In seguito solo le forze di polizia stradale intervenute potranno attivarsi per ottenere le immagini ed i dati dell'evento, fornendo agli interessati solo quanto necessario per soddisfare interessi legittimi non altrimenti raggiungibili.

9.In tutti i casi di eventi ripresi da sistemi di videosorveglianza comunali che possano configurare violazioni amministrative o reati il cittadino dovrà rivolgersi al competente servizio di polizia affinché sia questo a richiedere le immagini ed i dati necessari (ad es. danneggiamento di cose senza individuazione del responsabile, o simili casistiche).

10. Nell'ambito delle investigazioni difensive, il difensore della persona sottoposta alle indagini, a norma dell'Art. 391-quater c.p.p., può acquisire copia delle riprese in formato digitale dei filmati della videosorveglianza presentando specifica richiesta scritta e motivata al Designato previo pagamento anticipato delle relative spese. Salvo l'ipotesi di conservazione per diverse finalità, i dati si intendono disponibili per i normali tempi di conservazione. Se i supporti informatici con le immagini richieste non saranno ritirate entro 7 giorni dalla comunicazione all'interessato della disponibilità saranno eliminati in forma permanente e non recuperabile.

11. Il cittadino vittima o testimone di reato, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, può richiedere che i filmati siano conservati oltre i termini di Legge - come dispone il comma 6 del presente articolo - per essere messi a disposizione dell'organo di polizia procedente. La richiesta deve comunque pervenire entro i termini di conservazione previsti. La polizia locale, nell'immediatezza, potrà bloccare la cancellazione delle immagini d'interesse del privato cittadino solo nel caso fosse necessario attendere i tempi di proposizione denuncia/querela o altri adempimenti che prevedono tempi di più lunghi di quelli di cancellazione dei dati. Spetterà all'organo di polizia coinvolto per le indagini procedere a formale richiesta di acquisizione dei filmati e tale richiesta deve pervenire entro 1 mese dalla data di presentazione della denuncia/querela, decorsi i quali i dati non saranno ulteriormente conservati.

12. Strutture interne comunali, altri Enti pubblici, organi di protezione civile, soccorso civile o sanitario, dovranno presentare richiesta scritta e motivata, su carta intestata, per ottenere dati/immagini e sarà cura del Designato valutare in merito alla possibilità di evasione, nel rispetto delle disposizioni contenute nel presente regolamento.

13. Per Strutture interne ed Enti si osserveranno le diposizioni di cui al comma 8 del presente articolo.

14. In ogni caso di accoglimento delle richieste di cui ai commi precedenti, l'addetto incaricato dal Designato dovrà tenere traccia delle operazioni eseguite al fine di acquisire i filmati e riversarli su supporto digitale con lo scopo di garantire la genuinità dei dati stessi.

15. l'Amministrazione Comunale disporrà per il recupero delle spese necessarie a soddisfare le esigenze dei privati cittadini, avvocati e compagnie assicuratrici, individuando, con delibera di Giunta Comunale, una somma che comprenda tutte le spese sostenute per fornire quanto richiesto (personale, tempo di lavoro impiegato, supporti informatici, etc.), tale somma dovrà essere versata prima di ritirare il materiale richiesto. Per ciò che potrà essere fornito all'Autorità Giudiziaria, a Forze di Polizia e polizia locale di altri comuni la

Giunta Comunale potrà deliberare un limite di spesa oltre il quale i richiedenti dovranno pagare per la fornitura di quanto richiesto. Per quanto concerne ciò che potrà essere fornito ad altri Enti pubblici, organi di protezione civile, soccorso civile o sanitario la Giunta Comunale potrà deliberare specifiche esenzioni e/o le somme per le spese sostenute e che dovranno essere pagate prima di ritirare il materiale richiesto.
16. La polizia locale potrà dotarsi ed avvalersi di moduli specifici da fornire ai richiedenti per la presentazione delle richieste di cui al presente articolo.

CAPO VII
DISPOSITIVI DI VIDEOSORVEGLIANZA

Art. 35
Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada.

1. Gli impianti di rilevamento automatizzato delle infrazioni, utilizzati per documentare la violazione delle disposizioni in materia di circolazione stradale, analogamente all'utilizzo di sistemi di videosorveglianza, comportano un trattamento di dati personali.

2. L'utilizzo di tali sistemi è lecito solo in relazione alle violazioni che le norme prevedono possano essere rilevate anche attraverso sistemi di videosorveglianza (apparecchiature omologate/approvate per specifiche violazioni di norma del C.d.S.) e, in ogni caso, sono raccolti esclusivamente dati pertinenti e non eccedenti per il perseguimento delle finalità istituzionali del titolare, delimitando a tal fine la dislocazione e l'angolo visuale delle riprese in modo da non raccogliere immagini non pertinenti o inutilmente dettagliate. In conformità alla prassi ed al quadro normativo di settore riguardante talune violazioni del C.d.S., la normativa vigente in materia di protezione dei dati personali prescrive quanto segue:

a) gli impianti elettronici di rilevamento devono circoscrivere la conservazione dei dati alfanumerici contenuti nelle targhe automobilistiche ai soli casi in cui risultino non rispettate le disposizioni in materia di circolazione stradale;

b) le risultanze fotografiche o le riprese video possono individuare unicamente gli elementi previsti dalla normativa di settore per la predisposizione del verbale di accertamento delle violazioni (es., ai sensi dell'art. 383 del D.P.R. n. 495/1992, il tipo di veicolo, il giorno, l'ora e il luogo nei quali la violazione è avvenuta); deve essere effettuata una ripresa del veicolo che non comprenda o, in via subordinata, mascheri, per quanto *possibile, la porzione delle risultanze video/fotografiche riguardanti soggetti non coinvolti nell'accertamento* amministrativo (es., pedoni, altri utenti della strada);

c) le risultanze fotografiche o le riprese video rilevate devono essere utilizzate solo per accertare le violazioni delle disposizioni in materia di circolazione stradale anche in fase di contestazione, ferma restando la loro accessibilità da parte degli aventi diritto;

d) le immagini devono essere conservate per il periodo di tempo strettamente necessario in riferimento alla contestazione, all'eventuale applicazione di una sanzione e alla definizione del possibile contenzioso in conformità alla normativa di settore, fatte salve eventuali esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria;

e) le fotografie o le immagini che costituiscono fonte di prova per le violazioni a norme del c.d.s. non devono essere inviate d'ufficio al domicilio dell'intestatario del veicolo unitamente al verbale di contestazione, ferma restando la loro accessibilità agli aventi diritto;

f) in considerazione del legittimo interesse dell'intestatario del veicolo di verificare l'autore della violazione e, pertanto, di ottenere dalla competente autorità ogni elemento a tal fine utile, la visione della documentazione video-fotografica deve essere resa disponibile a richiesta del destinatario del verbale; al momento dell'accesso, dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo.

3. Solo nel caso di incidenti stradali le immagini ed i dati raccolti possono essere utilizzati per rilevare qualsiasi violazione alle norme del C.d.S. (art. 13, legge 24 novembre 1981, n. 689).

4. Possono altresì essere raccolte immagini relative a qualsiasi violazione a norme C.D.S. solo per supportare e/o dimostrare gli elementi oggettivi di riscontro che l'accertatore ha rilevato, così come dispone l'art. 13 della L. 689/81 e s.m.i. (ad esempio: veicolo in sosta irregolare, mancata esposizione "disco orario"/tagliando pagamento sosta, contrassegno disabili/"permesso rosa", mancato rispetto delimitazione stalli, ect.).

Art. 36
Utilizzi particolari - Z.T.L.- A.P. - Centri storici – Z.P.R.U.

1.Qualora il sistema di videosorveglianza venga utilizzato a fini di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato e zone di particolare rilevanza urbanistica, si dovrà rispettare quanto dettato dal D.P.R. 22 giugno 1999, n. 250. Tale normativa impone al titolare del trattamento dei dati di limitare la raccolta dei dati sugli accessi rilevando le immagini solo in caso di infrazione (art. 3 D.P.R. n. 250/1999). In questo specifico caso e utilizzo, i dati trattati potranno essere conservati solo per il periodo necessario per contestare le infrazioni e definire il relativo contenzioso e si potrà accedere ad essi solo a fini di polizia giudiziaria o di indagine penale.

2. In caso di rilevazione immediata e diretta su strada da parte degli organi accertatori di cui all'art. 12 c.d.s. di accessi irregolari sarà possibile che questi fotografino/riprendano i veicoli nel rispetto dell'art. 13 della L. 689/81.

Art. 37
Abbandono e conferimento dei rifiuti.

1. In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza fissi e/o mobili risulta consentito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e/o di sostanze pericolose laddove non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.
2. Analogamente, l'utilizzo di sistemi di videosorveglianza - sia fissi che mobili - sarà lecito laddove risultano inefficaci o inattuabili altre misure, nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13, legge 24 novembre 1981, n. 689).

Art. 38
Utilizzo di particolari videocamere mobili: Body Cam, Dash Cam, dispostivi di telefonia mobile, droni.

1. Per specifiche finalità concernenti la tutela dell'ordine e della sicurezza urbana e pubblica, la prevenzione, l'accertamento e la repressione dei reati e per rilevare o avere prova di violazioni amministrative - laddove le norme lo consentano -, gli operatori di Polizia Locale possono essere dotati di sistemi di microtelecamere da indossare sulla divisa - “body cam” - e sui veicoli in dotazione - “dash cam” - per l’eventuale ripresa di situazioni di criticità per la sicurezza propria e altrui.
2. Gli operatori di Polizia Locale possono utilizzare, nelle condizioni in cui ritengono possa esserci rischio o necessità di avere traccia video/sonora dell’attività che andranno a svolgere, delle **Body Cam** e/o delle **Dash Cam** in conformità delle indicazioni dettate dal Garante della Privacy con nota 26 luglio 2016, prot. n. 49612, ed al parere preventivo pubblicato il 31/7/2014 (docweb 3423775) 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". Possono essere utilizzati anche i **dispositivi di telefonia mobile** forniti in dotazione dall’Ente o, all’occorrenza, di proprietà degli operatori di Polizia Locale, per le stesse finalità delle bodycam secondo apposito disciplinare.
3. Il trattamento dei dati personali effettuati con simili sistemi di ripresa devono rispettare i principi di cui all’art. 5 del Regolamento Europeo sulla privacy e della Direttiva UE 2016/680 ed 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 o distrutti.
4. i sistemi A.P.R. - aeromobili a pilotaggio remoto o U.A.S. - in italiano: aeromobili senza equipaggio - potranno essere utilizzati solo quando le norme lo consentiranno, superando il divieto d’utilizzo da parte dei comuni, e segnatamente della polizia locale, imposto con **Decreto Ministero dell’interno del 13/6/22** “modalità di utilizzo da parte delle forze di polizia degli aeromobili a pilotaggio remoto”. intendersi anche e non solo arerei ma terrestri o acquatici Altri sistemi a pilotaggio remoto terrestri e/o acquatici potranno essere utilizzati solo rispettando le specifiche norme in materia.

Art. 39
Foto trappole.

1. Gli apparati “**videocamere mobili o dispositivi ricollocabili**” (foto trappole) vengono posizionati secondo necessità, esclusivamente nei luoghi teatro di illeciti penali o amministrativi, quando questi ultimi 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.

Art. 40
Utilizzo in ambienti di lavoro.

1. Ai sensi di quanto previsto dall’articolo 4 della Legge 20 maggio 1970, n. 300, gli impianti di videosorveglianza e gli strumenti di rilevazione di dati di geolocalizzazione non possono essere utilizzati per effettuare controlli sull’attività lavorativa dei dipendenti dell’Ente, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.
2. Qualsiasi utilizzo di sistemi in ambienti di lavoro deve soddisfare i principi di liceità, non eccedenza e proporzionalità.
3. Il Titolare deve quindi attivarsi, in caso di necessità, per l’attuazione di misure di garanzia ai sensi dello Statuto dei Lavoratori.

CAPO VIII
GESTIONE DEL DATA BREACH.

Art. 41
Perdita dei dati – Data Breach.

1. Il personale che provvede al concreto utilizzo dei dispositivi di videosorveglia, dovrà segnalare immediatamente al Designato dell'Ente, qualsiasi anomalia, malfunzionamento, nonché la perdita – anche parziale – accidentale o volontaria di dati (Data Breach).

Art. 42
Gestione della comunicazione del Data Breach.

1. Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato, sotto la supervisione del DPO.
2. In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.
3. Nel caso in cui una delle figure abilitate al trattamento si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente informare dell'incidente il superiore gerarchico, congiuntamente ne daranno comunicazione al titolare del trattamento mediante segnalazione scritta e dettagliata dell'evento, seguendo quanto dispone il successivo articolo 43. La stessa segnalazione verrà inviata a mezzo mail o PEC all'indirizzo del DPO.

Art. 43
Identificazione e indagine preliminare.

1. La segnalazione permetterà al Titolare del trattamento insieme al DPO, di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con il risk assessment (step 2) e con il coinvolgimento dell'Autorità garante per la Protezione dei dati.
2. Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare del trattamento insieme al DPO dovrà coinvolgere anche il Responsabile dell'Ufficio IT o un suo delegato in caso di assenza.
3. Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nella segnalazione, quali:
a) la data di scoperta della violazione (tempestività);
b) Il soggetto che è venuto a conoscenza della violazione;
c) la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
d) le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
e) la descrizione di eventuali azioni già poste in essere.

Art 44
Contenimento, Recovery e risk assessment.

1. Il Titolare del trattamento o un suo delegato insieme al DPO dovranno stabilire:
a) se esistono azioni che possano limitare i danni che la violazione potrebbe causare (ad esempio: riparazione fisica di strumentazione, utilizzo dei file di back up per recuperare dati persi o danneggiati, isolamento/chiusura di un settore compromesso della rete, cambio dei codici di accesso, etc.);
b) una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
c) se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati Personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
d) se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).
2. Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento e il DPO valuteranno la gravità della violazione utilizzando il Modulo di valutazione del Rischio connesso al Data Breach (disponibili sul sito dell'Autorità garante della protezione dei dati) che dovrà essere esaminato, unitamente al modulo di cui art. 37 del GDPR tenendo, altresì, in debita considerazione i principi e le indicazioni di cui all'art. 33 del GDPR .
3. Se, infatti, gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio semplice, l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio elevato.

Art. 45
Eventuale notifica all'Autorità Garante competente.

1. Una volta valutata la necessità di effettuare notifica della violazione dei dati subita, secondo quanto prescritto dal Regolamento (UE) 2016/679, (Denominazione dell'ente) dovrà provvedervi, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.
2. Pertanto, il Titolare del trattamento e il DPO invieranno la corretta modulistica all'Autorità Garante per la protezione dei dati personali così da effettuare la notificazione del data breach.

Art. 46
Eventuale comunicazione agli interessati.

1. Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati agli interessati, secondo quanto prescritto dal Regolamento (UE) 2016/679, l'Ente dovrà provvedervi, senza ingiustificato ritardo.
2. Quanto al contenuto di tale comunicazione, il Titolare del trattamento e il DPO dovranno:
a) comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
b) descrivere le probabili conseguenze della violazione dei dati personali;
c) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.
3. Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento e il DPO dovranno sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali e-mail, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Art. 47
Documentazione della violazione.

1. Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente, l'Ente sarà tenuto a documentarlo su apposito registro.
2. Tale documentazione sarà affidata al Titolare del trattamento o da un suo delegato con l'ausilio del Responsabile dell'Ufficio I.T. (qualora la violazione riguardi dati contenuti in sistemi informatici) vi provvederà mediante la tenuta del Registro dei Data Breach, secondo le informazioni ivi riportate:
a) numero della violazione;
b) data violazione;
c) natura della violazione;
d) categoria di interessati;
e) categoria di dati personali coinvolti;
f) numero approssimativo di registrazioni dei dati personali;
g) conseguenze della violazione;
h) contromisure adottate;
i) se sia stata effettuata notifica all'Autorità Garante Privacy;
j) se sia stata effettuata comunicazione agli interessati.
3. Il Registro dei Data Breach deve essere continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.

CAPO IX
TUTELA AMMINISTRATIVA E GIURISDIZIONALE – MODIFICHE.

Art. 48
Tutela.

1. Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss. del RGPD ed alle disposizioni attuative e dagli artt. 37 e ss. del D. Lgs. 51/2018 relativo 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.
2. In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4-6 della legge 7 agosto 1990, n. 241, è il designato al trattamento dei dati personali.

Art. 49
Modifiche regolamentari - Rinvio dinamico.

1. I contenuti del presente regolamento si devono adeguare nei casi di aggiornamento normativo in materia di trattamento dei dati personali o normative sovraordinate. Gli eventuali atti normativi, atti amministrativi dell'Autorità di tutela della privacy o atti regolamentari generali del Consiglio comunale dovranno essere celermente recepiti.
2. Le disposizioni del presente regolamento si intendono comunque modificate per effetto di sopravvenute norme vincolanti statali, regionali o quant'altro le ponga in contrasto o incompatibili con le nuove disposizioni. Lo stesso dicasi per le tecnologie sopraggiunte che rendano superati i richiami presenti nel regolamento; pertanto dovranno ritenersi aggiornati allo stato dell'arte.
3. In tali casi, in attesa della formale modificazione del presente regolamento, si applica la normativa sovra ordinata o la tecnologia sopraggiunta.

Art. 50
Danni cagionati per effetto del trattamento di dati personali.

1.Chiunque subisca un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento ai sensi delle disposizioni di cui all'art. 82, RGPD.
2. Il titolare o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
3. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2, RGPD.

CAPO X
DISPOSIZIONI FINALI.

Art. 51
Parternariato pubblico privato per il potenziamento della videosorveglianza ad uso pubblico. Sistemi integrati di trattamento dei dati.

1. Il Comune può promuovere ed attuare, per la parte di competenza, il coinvolgimento dei privati per la realizzazione di singoli punti di videosorveglianza, orientati comunque su vie ed aree pubbliche o di uso pubblico, nel rispetto dei principi di cui al presente Regolamento.
2. I privati interessati assumono su di sé ogni onere per:
a) acquistare le attrezzature e renderle operative, con connessione al sistema centrale presso il comando di polizia locale in conformità alle caratteristiche tecniche dell'impianto comunale o di un modello compatibile;
b) metterle a disposizione del Comune a titolo gratuito, senza mantenere alcun titolo di ingerenza sulle immagini e sulla tecnologia connessa.
3. Il Comune assume su di sé gli oneri per la manutenzione periodica e la responsabilità della gestione dei dati raccolti.
4. In accordo con il Comune, e mediante la stipula di apposita convenzione/accordo, i soggetti privati che hanno ceduto i propri impianti di videosorveglianza al Comune potranno decidere di affidare il controllo diretto delle telecamere a istituti di vigilanza privata, anche prevedendo l'installazione dell'impianto presso una *controll room* dedicata collegata con il comando di Polizia Locale. Gli oneri finanziari dell'affidamento di tale servizio ricadranno sul soggetto privato che, una volta individuato l'istituto di vigilanza privata cui affidare il servizio, ne comunicherà il nominativo al Comune.
5. Spetterà poi al Comune, in qualità di titolare del trattamento dati derivanti dal sistema di videosorveglianza procedere ai sensi di legge a tutti gli atti conseguenti e alla nomina del responsabile del trattamento dati e al conferimento ai singoli operatori dell'istituto di videosorveglianza individuati dei compiti e dei ruoli necessari allo svolgimento del servizio.
6. In ottemperanza ai principi di economicità delle risorse e dei mezzi impiegati, previo accordo scritto con gli Organi interessati, è possibile il ricorso a sistemi integrati di trattamento dei dati tra diversi soggetti, pubblici e privati.
7. Nell´ambito dei predetti trattamenti, sono individuabili le seguenti tipologie di sistemi integrati:
a) gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, dei dati da parte di diversi e autonomi titolari del trattamento, i quali utilizzano le medesime infrastrutture tecnologiche; in tale ipotesi, i singoli titolari possono trattare i dati solo nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali ed alle finalità chiaramente indicate nell´informativa, nel caso dei soggetti pubblici, ovvero alle sole finalità riportate nell´informativa, nel caso dei soggetti privati;
b) collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo; tale soggetto terzo, designato responsabile del trattamento ai sensi dell´art. 28 RGPD da parte di ogni singolo Titolare, deve assumere un ruolo di coordinamento e gestione dell´ attività di trattamento senza consentire, tuttavia, forme di correlazione dei dati per conto di ciascun Titolare;
c) sia nelle predette ipotesi, sia nei casi in cui l´attività di trattamento venga effettuata da un solo Titolare, si può anche attivare un collegamento dei sistemi di gestione con le sale o le centrali operative degli organi di polizia. L´ attivazione del predetto collegamento deve essere reso noto agli interessati.
8. Le modalità di trattamento sopra elencate richiedono l´adozione di specifiche misure di sicurezza, quali:
a) adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all´esercizio dei doveri di verifica periodica dell´operato dei responsabili da parte del Titolare, comunque non inferiore a sei mesi;
b) separazione logica dei dati registrati dai diversi titolari.
9.Fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di trattamento abbiano natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il Titolare del trattamento può effettuare una valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD.

Art. 52
Tutela dei dati personali - Valutazione di impatto sulla protezione dei dati.

1. Il comune garantisce, nelle forme ritenute più idonee, che il trattamento dei dati personali in suo possesso si svolge nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, ai sensi delle vigenti disposizioni in materia.

2. In ossequio al disposto di cui all'art. 35 RGPD, qualora il trattamento di dati realizzato mediante i sistemi oggetto del presente Regolamento possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare provvederà - previa consultazione con il Responsabile della Protezione dei Dati - all' effettuazione di una valutazione di impatto sulla protezione dei dati personali.
3. Il Titolare del trattamento, prima di procedere al trattamento, consulta l'Autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 RGPD indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio.
4.La valutazione di impatto non verrà effettuata qualora il trattamento dovesse rientrare nell'elenco delle tipologie di trattamenti, redatto dal Garante della Privacy, per le quali non è richiesta.

Art. 53
Entrata in vigore.

1. Il presente Regolamento entrerà in vigore con il conseguimento della esecutività o della dichiarazione di immediata eseguibilità della deliberazione di approvazione, secondo le leggi vigenti ed osservate le procedure dalle stesse stabilite.
2. Il presente regolamento abroga ogni disposizione regolamentare precedente che disciplina tale materia.
3. Per quanto non disciplinato dal presente Regolamento si rinvia al D. Lgs. 196/2003 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, al RGPD e al D. Lgs. 51/2018 relativo 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 ai provvedimenti generali sulla videosorveglianza approvati dall'Autorità Garante per la protezione dei dati personali e alle indicazioni centrali del Ministero dell'Interno.