CITTÀ DI VITTORIA

REGOLAMENTO PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA

INDICE

CAPO VII - NORME FINALI

CAPO I
- DISPOSIZIONI GENERALI -

Art. 1 – Finalità

1. Il presente Regolamento disciplina il trattamento dei dati personali acquisiti mediante la videosorveglianza e le modalità di gestione dei relativi impianti e procedimenti amministrativi connessi.
2. Garantisce altresì che il trattamento dei dati personali, effettuato mediante l'attivazione di un impianto di videosorveglianza nel territorio del Comune di Vittoria, gestito ed utilizzato dal Corpo di Polizia Municipale e qualora richiesto, dall'Autorità di Pubblica Sicurezza o Giudiziaria, venga gestito per lo svolgimento delle funzioni istituzionali, per la tutela della sicurezza urbana, per attività di indagine e comunque nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. Disciplina, inoltre, le modalità di collegamento al sistema pubblico da parte di soggetti privati.
3. In particolare il presente regolamento:
a) individua gli impianti di videosorveglianza di proprietà del Comune di Vittoria da esso gestiti attraverso apposita determinazione del responsabile della gestione dell'impianto;
b) definisce le caratteristiche e le modalità di utilizzo degli impianti di videosorveglianza;
c) disciplina gli adempimenti, le garanzie e le tutele per il legittimo e pertinente trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza.
4. Garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento e le modalità di accesso ai dati.

Art. 2 – Definizioni

1. Ai fini del presente Regolamento si intende:
   a) per "banca dati" o "archivio", il complesso di dati personali, formatosi presso la centrale operativa della Polizia Municipale, raccolti esclusivamente mediante riprese videoregistrate, che in relazione ai luoghi di installazione delle videocamere interessano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto eventuali;
   b) per "trattamento", tutte le operazioni svolte con l'ausilio di mezzi elettronici, o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la cancellazione e la distruzione di dati;
   c) per "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, e rilevati con trattamenti di immagini effettuati attraverso l'impianto di videosorveglianza;
   d) per "titolare", l'ente Comune di Vittoria, nella persona del Sindaco cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali;
   e) per "cotitolare", i responsabili dell' autorità di Pubblica Sicurezza o Giudiziaria e comunque degli enti che hanno possibilità di trattamento dei dati ed a cui competono le decisioni in ordine alle modalità del citato trattamento dei dati personali per quanto di specifica competenza;
   f) per "responsabile", la persona fisica, legata da rapporto di servizio al titolare e preposto dal medesimo al trattamento di dati personali ovvero individuato anche in assenza di rapporto di servizio ma all'uopo incaricato dal titolare;
   g) per "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
   h) per "interessato" o "destinatario" la persona fisica, la persona giuridica, l'ente o associazione a cui si riferiscono i dati personali;
   i) per "terzo" la persona fisica, la persona giuridica, l'ente o associazione che non sia né interessato, incaricato o reponsabile dei dati o del trattamento;
   j) per "comunicazione", il dare conoscenza dei dati personali a soggetti determinati in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
   k) per "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
   l) per "dato anonimo", il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non possa essere associato ad un interessato identificato o identificabile;
   m) per "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
   n) per "amministratore di sistema" si individua, in ambito informatico, le figure professionali finalizzate alla gestione e alla manutenzione dell'impianto di videosorveglianza e per l'elaborazione delle sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei

rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi. Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente «responsabili» di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati. Attività tecniche quali il salvataggio dei dati (backup/ recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali;

o) per "responsabile della gestione tecnica" la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;

p) per "Responsabile della protezione dati" (DPO) il soggetto che per qualità professionali e conoscenze specialistiche della normativa e delle prassi in materia di protezione dei dati è in grado di svolgere le funzioni stabilite dalla sezione 4 del regolamento UE n 2016/679 pubblicato sulla Gazzetta Ufficiale Europea del 4 maggio 2016.

Art. 3 – Ambito di applicazione

1. Il presente Regolamento disciplina il trattamento di dati personali, realizzato mediante l'impianto di videosorveglianza, attivato sul territorio del Comune di Vittoria e collegato alla centrale operativa della Polizia Municipale, nonché eventualmente, se richiesto della Questura, dell'Arma dei Carabinieri, e della Guardia di Finanza, definisce le modalità di gestione dell'impianto e delle sale di controllo e dei procedimenti amministrativi inerenti le immagini registrate nonché delle altre forme di videosorveglianza con apparecchiature specificatamente omologate per l'accertamento delle sanzioni al codice stradale di cui al capo IV.

Art. 4 – Trattamento dei dati personali per le finalità istituzionali dell'impianto di videosorveglianza

1. Il trattamento dei dati personali è effettuato a seguito dell'attivazione di un impianto di videosorveglianza, i cui monitor per la visione delle immagini riprese dalle telecamere sono posizionati presso la centrale operativa e gli uffici della Polizia Municipale, e se attivato della Questura, dell'Arma dei Carabinieri, e della Guardia di Finanza.

2. L'utilizzo degli impianti di videosorveglianza è finalizzato a:

a) prevenire e reprimere atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, anche ai fini dell'acquisizione di elementi di prova al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" di cui all'art. 1 del decreto del Ministro dell'Interno 5 agosto 2008 e dell'art. 2 della legge 18 aprile 2017 n° 48 nonché di ogni altro riferimento normativo in materia;

b) prevenire e reprimere fenomeni di degrado urbano e svolgere controlli volti ad accertare e sanzionare violazioni delle norme in materia ambientale e delle disposizioni del regolamento comunale per la raccolta differenziata dei rifiuti;

c) vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato, dell'ordine, del decoro e della quiete pubblica;

d) controllare determinate aree del territorio comunale anche a fini di protezione civile;

e) monitorare i flussi di traffico e ricostruire la dinamica dei sinistri stradali con feriti;

f) prevedere l'attivazione di misure di prevenzione e di tutela della pubblica sicurezza in ambito comunale;

g) garantire la ricostruzione, in tempo reale, della dinamica di atti vandalici o azioni di teppismo nei luoghi pubblici di principale frequentazione, per permettere un pronto intervento della Polizia Municipale e delle Forze dell'Ordine a tutela del patrimonio pubblico;

h) utilizzare apparecchiature omologate per l'accertamento delle infrazioni al codice stradale.

3. Le finalità del suddetto impianto devono essere conformi alle funzioni istituzionali demandate al Comune di Vittoria, nonché alle disposizioni legislative e regolamentari in vigore, oltre che allo Statuto e ai Regolamenti Comunali.

4. L'utilizzo degli impianti di videosorveglianza da parte del Corpo di Polizia Municipale, dell'Autorità di Pubblica Sicurezza o Giudiziaria, costituisce inoltre uno strumento di prevenzione e di razionalizzazione dell'azione di Polizia Municipale, Polizia di Stato, Carabinieri e Guardia di Finanza sul territorio comunale, a seguito delle intese e dei patti di sicurezza e coordinamento del territorio.

5. Il sistema di videosorveglianza comporterà esclusivamente il trattamento di dati personali, nell'ambito delle disposizioni di legge e del Garante della privacy, rilevati mediante le riprese video e che, in relazione ai luoghi

di installazione delle videocamere, interesseranno soggetti ed i mezzi di trasporto che transiteranno nell'area videosorvegliata.
6. L'attività di videosorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza oltre che di liceità della raccolta dati effettuata per finalità esclusivamente di interesse pubblico o sancite da disposizioni di legge e di esercizio di pubblici poteri. Viene esplicitamente escluso l'utilizzo del sistema per regolazione di attività tra soggetti privati o terzi.
La localizzazione delle telecamere e le modalità di ripresa saranno quindi stabilite in modo conseguente.
7. Gli impianti di videosorveglianza non possono essere utilizzati per l'irrogazione di sanzioni per infrazione al Codice della Strada, ma esclusivamente per l'eventuale invio, da parte delle Centrali Operative, di personale con qualifica di organo di Polizia Stradale per le contestazioni ai sensi del Codice della Strada o per l'utilizzo ai fini giudiziari in caso di reati o sinistri stradali con esiti lesivi. L'irrogazione di sanzioni è ammessa solo per gli impianti appositamente omologati per tale scopo.
8. La possibilità di disporre in tempo reale di dati ed immagini costituisce un ulteriore strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Municipale e le Forze dell'Ordine svolgono quotidianamente nell'ambito delle proprie competenze istituzionali; attraverso tali strumenti si persegue l'intento di tutelare la popolazione ed il patrimonio privato e comunale, garantendo quindi un elevato grado di sicurezza nei luoghi di maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, artistico e culturale, negli edifici pubblici, nel centro storico, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare e comunque il tutto finalizzato per ottenere maggiore efficienza nella prevenzione e repressione dei reati e di ogni comportamento non conforme alla legalità.
9. L'uso dei dati personali nell'ambito di cui trattasi non necessita del consenso degli interessati in quanto viene effettuato per lo svolgimento di funzioni istituzionali che sono assoggettate alla normativa vigente in materia di "privacy" con apposita regolamentazione. A tal scopo è tassativamente esclusa la possibilità di accesso diretto ai dati della videosorveglianza da parte dei privati cittadini ad eccezione di quelli inerenti le apparecchiature omologate per l'accertamento delle infrazioni stradali.
10. L'impianto di videosorveglianza non potrà essere utilizzato, in base all'art. 4 dello Statuto dei lavoratori (legge n° 300 del 20 maggio 1970) per effettuare controlli sull'attività lavorativa dei dipendenti dell'Amministrazione comunale, di altre Amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati. Gli impianti di videosorveglianza non potranno essere utilizzati per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati, per finalità di promozione turistica o per finalità di analisi storica. Potranno essere collocati impianti all'interno degli edifici che risultino sede di luogo lavorativo solo previo assenso esplicito delle rappresentanze sindacali.
11. I dati del sistema di videosorveglianza cittadina, ad eccezione di quelli utilizzati per il controllo dei varchi delle zone a traffico limitato, sono comunque acquisiti nel rispetto e con le modalità stabilite dal D.lgs. n° 51 del 18 maggio 2018 concernente il trattamento dei dati personali ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali e quindi dalla direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016.

Art. 5 – Notificazione preventiva al garante

1. I dati trattati devono essere notificati al Garante solo se rientrano nei casi specificatamente previsti dalla normativa vigente sulla privacy. A tale proposito la normativa prevede che non vadano comunque notificati i trattamenti relativi a comportamenti illeciti o fraudolenti, quando riguardino immagini conservate temporaneamente per esclusive finalità di sicurezza pubblica o di tutela delle persone e del patrimonio.
2. Il trattamento dei dati personali si svolge nel pieno rispetto dei principi di liceità, finalità, necessità e proporzionalità e delle finalità previste dal regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio approvato il 27 aprile 2016 ed in attuazione di tali principi il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza è effettuato dal Comune di Vittoria e dagli altri contitolari indicati nel presente regolamento esclusivamente per lo svolgimento delle funzioni istituzionali e per il perseguimento delle finalità di cui all'articolo 4.
3. In attuazione del principio di necessità, gli impianti di videosorveglianza ed i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere raggiunte mediante dati anonimi od opportune 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. Tutti i dati raccolti vengono conservati entro i termini di legge e comunque cancellati e distrutti nel momento in cui cessi la finalità che ne consente il trattamento.

CAPO II
- SOGGETTI -

Art. 6 – Titolare trattamento dei dati

1. Il Comune di Vittoria è titolare del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento. A tal fine il Comune di Vittoria è rappresentato dal Sindaco, a cui compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza.
2. Il Sindaco, in qualità di rappresentante dell'Ente è titolare del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza e provvede:

a) a definire le linee organizzative per l'applicazione della normativa di settore;
b) ad effettuare le notificazioni al Garante per la protezione dei dati personali se dovute;
c) alla nomina dei responsabili della gestione tecnica degli impianti di videosorveglianza, dei responsabili del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza, del responsabile per la protezione dei dati, impartendo istruzioni ed assegnando compiti e responsabilità;
d) a dettare le linee guida di carattere fisico, logico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza;
e) a vigilare sulla puntuale osservanza delle disposizioni impartite.

Art. 7 – Contitolare trattamento dei dati

1. I responsabili delle altre forze di Polizia, o comunque i legali rappresentanti di altri enti connessi al sistema di videosorveglianza sono Contitolari del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di cui al presente regolamento. A tal fine le citate strutture sono rappresentate dai corrispondenti responsabili pro-tempore, cui competono le decisioni circa le modalità del trattamento, ivi compreso il profilo della sicurezza, nonché tutte le attività e compiti di cui all'art. 6, 2° comma, del presente regolamento.
2. I responsabili di cui al punto precedente, in qualità di contitolare del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza:

a) definiscono le linee organizzative per l'applicazione della normativa di settore per le strutture di propria competenza;
b) nominano i responsabili del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza, impartendo istruzioni ed assegnando compiti e responsabilità;
c) dettano le linee guida di carattere fisico, logico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza;
d) vigilano sulla puntuale osservanza delle disposizioni impartite;
e) inviano al Comune copia dei provvedimenti indicati ai punti precedenti.

Art. 8 – Responsabile trattamento dei dati

1. Nell'ambito del Comune il Responsabile del trattamento dati per il profilo della gestione del servizio è individuato nell'Ufficiale della Polizia Municipale che gestisce il servizio/sistema di videosorveglianza comunale (ovvero il Comandante o altro ufficiale di polizia municipale) ed è incaricato, previa nomina da effettuare con atto del Sindaco, quale Responsabile del trattamento dei dati personali rilevati. È consentito il ricorso alla delega scritta di funzioni da parte del designato, previa approvazione del Sindaco.
2. Il responsabile ha l'obbligo di attenersi a quanto previsto dalla normativa vigente in tema di trattamento dei dati personali, ivi incluso il profilo della sicurezza, alle istruzioni impartite dal Titolare e alle disposizioni del presente Regolamento.
3. Il Responsabile procede al trattamento attenendosi sistematicamente alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni previste dalla normativa vigente sulla privacy e su quelle indicate nelle proprie istruzioni.

4. I compiti affidati al Responsabile devono essere specificati per iscritto, in sede di designazione. Il Responsabile impartisce istruzioni operative agli incaricati e vigila sul loro operato.
5. Gli incaricati del materiale trattamento, nominati dal Sindaco, di concerto con il Responsabile, devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del Titolare o del Responsabile.
6. La visione delle immagini registrate e lo spostamento della direzione di registrazione delle telecamere sono consentiti solamente al Responsabile del trattamento dei dati, al suo delegato, agli incaricati preposti alla centrale operativa o a funzioni di polizia giudiziaria, ed al personale esterno addetto alla manutenzione ed alle riparazioni, quest'ultimo sempre previa autorizzazione del Responsabile.
7. Il Responsabile del trattamento dei dati impartisce idonee istruzioni atte ad evitare assunzioni o rilevamento non autorizzato di dati da parte delle persone abilitate all'accesso per la manutenzione e riparazione degli impianti.
8. Il Responsabile custodisce le chiavi per l'accesso ai locali della centrale operativa della Polizia Municipale, le chiavi degli armadi per la conservazione dei supporti informatici e le parole chiave per l'utilizzo dei sistemi in luogo sicuro e protetto.

Art. 9 – Responsabile della Protezione dei Dati (RPD)

1. Il Titolare e/o il Responsabile del trattamento designano un Responsabile della Protezione dei Dati (DPO) individuato in dipendente del Comune o in soggetto esterno all'Ente che per qualità professionali garantisca valide capacità e conoscenze specialistiche in materia.
2. Il Responsabile della protezione dati, oltre ai compiti indicati nella normativa europea e nazionale, deve valutare ed esaminare i rischi che comportano l'utilizzo dei sistemi di videosorveglianza nonché fornire consulenza in materia.
3. Il responsabile della protezione dati deve cooperare con le autorità di controllo e fungere da contatto con tali autorità.
4. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento dei sistemi di videosorveglianza.
5. Il responsabile della protezione dei dati non deve essere esclusivamente adibito ai compiti indicati nel presente regolamento ma agire nell'ambito più generale della normativa in materia di privacy ed i compiti a lui affidati concernono, oltre gli aspetti trattati nel presente regolamento, tutte le attività previste dalla sezione 4 del regolamento UE n° 2016/679.
6. **Per quanto concerne la videosorveglianza il R.P.D. deve informare e fornire consulenza al titolare del trattamento, ai contitolari ed al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento e dalla normativa comunitaria e nazionale in materia di protezione dei dati.**

Art. 10 – Responsabile esterno del trattamento dei dati

1. Il Titolare nomina un responsabile esterno del trattamento dei dati ogni qual volta un soggetto esterno è chiamato ad operare sui dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza comunale anche se applicando le direttive e sotto la supervisione del titolare stesso. La nomina è effettuata con decreto del Sindaco, nel quale sono analiticamente specificati i compiti affidati sulla base del rapporto intercorrente tra il soggetto esterno ed il Comune di Vittoria.
2. Tale responsabile esterno effettua il trattamento nel rispetto della normativa vigente in materia di protezione dei dati personali, ivi incluso il profilo della sicurezza, e delle disposizioni del presente regolamento.
3. Il responsabile effettua il trattamento attenendosi alle direttive impartite dal Titolare, il quale, anche tramite opportune verifiche, vigila sulla puntuale osservanza delle proprie disposizioni ed istruzioni.
4. Tale responsabile esterno individuato dal Sindaco, in collaborazione con il responsabile della gestione tecnica degli impianti di videosorveglianza ed il responsabile trattamento dei dati:
   a) adotta le misure e dispone gli interventi necessari per la sicurezza del trattamento dei dati e la correttezza dell'accesso ai dati;
   b) collabora con gli incaricati del trattamento dei dati personali;
   c) collabora con il titolare e il Responsabile della protezione dei dati per l'attuazione delle prescrizioni del Garante o delle Autorità di controllo.

Art. 11 – Responsabile della gestione tecnica degli impianti di videosorveglianza

1. Il dirigente del Servizio tecnico competente in materia informatica, o altro soggetto individuato dal Sindaco che abbia conoscenze specialistiche d'informatica e manutenzioni reti, è designato per il profilo manutentivo e tecnico informatico quale responsabile della gestione tecnica degli impianti di videosorveglianza di cui al presente regolamento. La nomina è effettuata con decreto del Titolare, nel quale sono analiticamente specificati i compiti affidati al responsabile. È consentito il ricorso alla delega scritta di funzioni da parte del soggetto designato, previa approvazione da parte del Titolare del trattamento.
2. Il dirigente del Servizio tecnico competente, o il diverso soggetto individuato dal Sindaco, in qualità di responsabile della gestione tecnica degli impianti di videosorveglianza:

a) cura l'installazione e gestisce la manutenzione degli impianti di videosorveglianza;
b) assegna e custodisce le credenziali di accesso necessarie per l'utilizzo degli impianti di videosorveglianza;
c) provvede al salvataggio periodico dei dati da conservare ed alla loro cancellazione scaduti i termini di conservazione nel rispetto delle istruzioni impartite a tal scopo dal Titolare del trattamento.

Art. 12 – Nomina degli incaricati alla gestione dell'impianto di videosorveglianza

1. Il Responsabile del trattamento dei dati designa e nomina gli incaricati in numero sufficiente a garantire la gestione del servizio di videosorveglianza nell'ambito degli addetti appartenenti al settore della Polizia Municipale.
2. Gli incaricati andranno nominati tra gli addetti alla Polizia Municipale e o tra i dipendenti in servizio presso il Comune di Vittoria che per esperienza, capacità ed affidabilità forniscano idonea garanzia nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.
3**. La gestione dell'impianto di videosorveglianza è riservata agli addetti di Polizia Municipale, aventi qualifica di Ufficiali ed Agenti di Polizia Giudiziaria ai sensi dell'art. 55 del Codice di Procedura Penale oppure ai dipendenti del Comune che siano nominati ai sensi di legge in qualità di ausiliari di Polizia Giudiziaria.**
4. Con l'atto di nomina, ai singoli incaricati, saranno affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi. In ogni caso, prima dell'utilizzo degli impianti, essi saranno istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento.

Art. 13 - Soggetti esterni

1. Ai soggetti esterni al Comune di Vittoria e dei quali l'Ente si avvale a qualsiasi titolo per lo svolgimento di servizi e attività per le quali si trattano dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento, si applicano le disposizioni inerenti le misure di sicurezza del presente regolamento. Nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele ed in particolare i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche; tale attività può essere svolta solo in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini.

Art. 14 – Persone autorizzate ad accedere alla centrale operativa della Polizia Municipale

1. L'accesso alla centrale operativa della Polizia Municipale è consentito solamente, oltre al titolare (Sindaco) o suo delegato, all'incaricato ed al personale autorizzato ai sensi del presente regolamento. Eventuali accessi di persone diverse da quelli innanzi indicate è severamente vietato durante il funzionamento del sistema di videosorveglianza oppure può essere autorizzato per specifiche esigenze dal Titolare o dal Responsabile con un'autorizzazione scritta, motivata e corredata da specifiche indicazioni in ordine ai tempi ed alle modalità dell'accesso.
2. L'accesso avviene in presenza di incaricati del Comune di Vittoria individuati ai sensi dell'articolo 12 del presente regolamento.
3. Possono essere autorizzati all'accesso alla centrale operativa della videosorveglianza presso la Polizia Municipale, durante i momenti in cui la stessa è in funzione, solo gli incaricati di servizi rientranti nei compiti istituzionali dell'ente di appartenenza o quelli che svolgano scopi connessi alle finalità di cui al presente Regolamento, nonché il personale addetto alla manutenzione degli impianti: durante il non funzionamento della videosorveglianza l'accesso è consentito senza limitazioni ma con opportune cautela atte a garantire l'inaccessibilità ai dati anche involontariamente.
4. Il Responsabile del trattamento dei dati 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, di pulizia dei locali o altro legittimo motivo.

5. Gli incaricati dei servizi di cui al presente Regolamento devono vigilare sul puntuale rispetto delle istruzioni e sulla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso alla centrale.
6. I dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono custoditi presso le centrali di controllo ubicate presso le sedi del Comune di Vittoria.

Art. 15 – Accesso ai sistemi e parola chiave

1. L'accesso ai sistemi informatici è esclusivamente consentito al Responsabile e agli incaricati con le modalità stabilite dal presente Regolamento.
2. Gli incaricati saranno dotati di propria password di accesso al sistema.
3. Il sistema dovrà essere fornito di "log" di accesso, che saranno conservati per la durata massima di un anno.

CAPO III
TRATTAMENTO DEI DATI PERSONALI

Art. 16 – Modalità di raccolta, conservazione e requisiti dei dati personali

1. I dati personali oggetto di trattamento e acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono:
   a) trattati in modo lecito e secondo correttezza;
   b) raccolti e registrati per le finalità di cui al presente regolamento e resi utilizzabili in altre operazioni di trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi e disciplinati dalla legge;
   c) esatti e, se necessario, aggiornati;
   d) trattati in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti e trattati, con modalità rivolte a salvaguardare l'anonimato anche successivamente alla fase della raccolta;
   e) i dati personali sono ripresi attraverso le telecamere dell'impianto di videosorveglianza;
   f) conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità per le quali sono raccolti e successivamente trattati ed in ogni caso per un periodo di tempo non superiore a sette giorni, fatte salve speciali esigenze di ulteriore conservazione per finalità di polizia giudiziaria o previa richiesta dell'Autorità Giudiziaria o a seguito di denunzia/querela penale; i dati indicati al capo IV vengono conservati sino alla conclusione dei procedimenti ad essi correlati; a tal scopo viene garantito espressamente il "diritto all'oblio" ovvero la possibilità da parte dell'interessato di richiedere la cancellazione e la cessazione di ogni trattamento dei dati che lo riguardano non più necessari per le finalità per le quali erano stati raccolti;
   g) non è prevista alcuna portabilità dei dati della videosorveglianza cittadina a favore degli interessati o soggetti terzi se non per esclusive finalità di tutela giudiziaria in ambito processuale dei propri interessi e previo consenso esplicito al trattamento da parte dei soggetti controinteressati.

2. Gli impianti di videosorveglianza di cui al presente regolamento consentono riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale oppure, in caso contrario, in bianco e nero. Di norma non sono effettuate riprese di dettaglio dei tratti somatici delle persone, a meno che non siano funzionali al soddisfacimento delle finalità di cui al presente regolamento ed effettuate per la prevenzione e repressioni di reati o atti illegali o illeciti.
3. I segnali video delle unità di ripresa sono inviati alle centrali di controllo ubicate presso le sedi del Comune di Vittoria, del Corpo di Polizia Municipale di Vittoria, e altresì, se richiesto, possono essere inviate alle centrali di controllo delle altre forze di Polizia. In queste sedi le immagini sono visualizzate su monitor e registrate su apposito server del Comune di Vittoria. Sul territorio comunale sono collocati, in appositi armadi sigillati, registratori ed ups per registrazioni da periferica. Per accedere a tali registrazioni è necessaria apposita password e le immagini vengono sovra registrate entro il termine di legge. L'impiego del sistema di videoregistrazione è necessario per ricostruire l'evento, ai fini del soddisfacimento delle finalità del presente regolamento.
4. Per accedere ai dati ed alle immagini, solo per finalità di giustizia, eventuali interessati non appartenenti alle forze di Polizia dovranno presentare un'apposita istanza scritta, adeguatamente motivata, diretta al Titolare o Contitolare del trattamento, corredata altresì dalla fotocopia del proprio documento di identità, richiedendo innanzitutto l'esistenza o meno del trattamento di dati che possano riguardarli; altresì potranno richiedere eventuali informazioni sugli estremi identificativi del Titolare e del Responsabile, sulle finalità e modalità del trattamento dei dati, sulla cancellazione, trasformazione in forma anonima o blocco dei dati trattati in violazione alla normativa vigente in materia; l'interessato potrà inoltrare la richiesta di opposizione al trattamento dei propri dati personali, per motivi legittimi e documentati, ancorché pertinenti alle finalità del trattamento.

5. Il Titolare e i responsabili del trattamento dei dati personali si obbligano a non effettuare delle riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto attivato.
6. I segnali video delle unità di ripresa della videosorveglianza fissa saranno sovrascritti decorsi i termini di legge (attualmente stabiliti in sette giorni) nonché registrati su server di monitoraggio e controllo ubicato presso la centrale operativa del Comando di Polizia Municipale o il Comune e presso le centrali di altre forze di Polizia.
In queste sedi le immagini saranno registrate su supporto magnetico da un sistema appositamente predisposto e visualizzate su monitor.
7. L'impiego del sistema di videoregistrazione si rende necessario per ricostruire le varie fasi dell'evento, nell'ambito delle finalità previste dal presente Regolamento.

Art. 17 - Conservazione dei dati personali

1. I dati personali registrati mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono conservati per un periodo di tempo non superiore a sette giorni dalla data della rilevazione ad eccezione di quelli indicati nel comma 5 e 6 del presente articolo. Decorso tale periodo, i dati registrati sono cancellati con modalità automatica.
2. La conservazione dei dati personali per un periodo di tempo superiore a quello indicato dal comma 1 del presente articolo è ammessa esclusivamente su specifica richiesta della Autorità Giudiziaria o di Polizia Giudiziaria in relazione ad un'attività investigativa in corso oppure su richiesta della cittadinanza nelle more della presentazione di denunzia all'Autorità. Le immagini videoregistrate sono conservate per speciali esigenze di ulteriore conservazione nei limiti e con le modalità stabilite al punto 3.4. Del provvedimento del Garante per la protezione dei dati personali dell'8 aprile 2010, ed in modo particolare, in relazione ad illeciti che si siano verificati o ad indagini delle autorità giudiziaria o di pubblica sicurezza.
3. Fuori delle ipotesi espressamente previste dal comma 2 del presente articolo, la conservazione dei dati personali per un tempo eccedente i sette giorni è subordinata ad una verifica preliminare del Garante per la protezione dei dati personali.
4. In relazione alle capacità di immagazzinamento dei dati forniti tramite i videoregistratori digitali, in condizioni di normale funzionamento, le immagini riprese in tempo reale distruggono quelle già registrate in un tempo inferiore a quello citato, in piena osservanza della normativa vigente sulla privacy.
5. Le riprese di eventuali telecamere posizionate ai varchi di eventuali Zone a Traffico Limitato sono disciplinate dal p.r. n° 250/1999 e la conservazione delle immagini viene mantenuta sino alla conclusione del procedimento sanzionatorio ad esso correlato.
6. Le riprese delle telecamere delle apparecchiature omologate finalizzate all'accertamento delle infrazioni al codice della strada ovvero le fotografie ed i video registrati per accertamenti sanzionatori, sia del codice stradale che per altri illeciti amministrativi o penali, sono conservati sino all'estinzione dell'obbligazione pecuniaria correlata al procedimento sanzionatorio o alla conclusione definitiva del procedimento penale.

Art. 18 – Obblighi degli operatori

1. L'utilizzo del brandeggio e dello zoom da parte degli operatori e degli incaricati al trattamento dovrà essere conforme alle finalità dell'impianto riportate nel presente regolamento.
2. Il settore di ripresa delle telecamere deve essere impostato in modo tale da consentire il controllo e la registrazione di quanto accada nei luoghi pubblici o aperti al pubblico, con esclusione tassativa delle proprietà private fatto salva specifica delega dell'Autorità Giudiziaria.
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 di cui al precedente articolo, solo in caso di effettiva necessità per il conseguimento delle finalità di cui all'articolo 4, comma 3 e a seguito di regolare autorizzazione di volta in volta richiesta al titolare del trattamento.
4. La mancata osservanza degli obblighi previsti al presente articolo 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. 19 - Informazioni rese al momento della raccolta (cartelli)

1. Il Comune di Vittoria, nei luoghi in cui sono posizionate le telecamere, affigge un'adeguata segnaletica su cui devono essere riportate le informazioni minime come previste dal punto 3.1 del provvedimento del garante in materia di videosorveglianza dell'08.04.2010 e dal nuovo regolamento Europeo sulla privacy GDPR 679/2016, mentre l'informativa completa viene resa ai sensi dell'art. 13 del citato GDPR a mezzo pubblicazione sul sito internet del Comune. Fermo quanto previsto dal presente comma il Comune di Vittoria rende noto agli interessati il funzionamento degli impianti di videosorveglianza installati all'interno di edifici comunali tramite posizionamento di cartelli contenenti l'informativa di legge.
2. Il cartello deve avere un formato ed un posizionamento tale da essere chiaramente visibile all'utenza e deve altresì inglobare il simbolo della telecamera ed essere posizionato nelle vicinanze del raggio di azione della videocamera.
3. Il cartello deve essere collocato anche in caso di posizionamento di telecamere mobili utilizzate ai fini sanzionatori con l'eccezione dell'utilizzo per fini di polizia giudiziaria.
4. Fermo quanto previsto dal comma 1 del presente articolo, il Comune di Vittoria rende noto agli interessati il funzionamento degli impianti di videosorveglianza tramite le seguenti forme semplificate di informativa:

a) pubblicazione sul sito internet istituzionale del presente regolamento e di ogni altra documentazione necessaria per obbligo di legge relativa alle zone videosorvegliate;
b) inserimento di appositi avvisi nella cartellonistica esistente in corrispondenza degli accessi stradali e ferroviari alla città.

Art. 20 – Diritti dell'interessato

1. In relazione al trattamento dei dati personali, è assicurato agli interessati, identificati o identificabili, l'effettivo esercizio dei propri diritti ed in particolare quello di accedere ai dati che li riguardano, di verificarne le finalità, le modalità del trattamento e di ottenerne l'interruzione nel caso di utilizzo illecito, in particolare per la carenza dell'adozione delle idonee misure di sicurezza o per l'uso indebito da parte di soggetti non autorizzati.
2. I diritti di cui al presente articolo riferiti a dati personali concernenti persone decedute, possono essere esercitati dagli eredi, da chi abbia un interesse proprio, da chi agisca a tutela dell'interessato o per ragioni familiari considerate particolarmente meritevoli di protezione.
3. Nell'esercizio dei diritti di cui ai commi precedenti 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. Le istanze di cui al presente articolo possono essere trasmesse al Titolare o al Responsabile anche mediante lettera raccomandata o posta elettronica, che dovrà provvedere in merito entro e non oltre trenta giorni.
5. Nel caso di esito negativo alle istanze di cui al presente articolo, 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.

Art. 21 – Procedura per l'accesso alle immagini da parte degli interessati

1. L'istanza deve altresì indicare a quale impianto di videosorveglianza si fa riferimento ed il giorno e l'ora in cui l'istante potrebbe essere stato oggetto di ripresa: nel caso tali indicazioni manchino, o siano insufficienti a permettere il reperimento delle immagini, di ciò dovrà essere data comunicazione al richiedente, così come nell'ipotesi in cui le immagini di possibile interesse non siano state oggetto di conservazione.
2. Il Responsabile del trattamento sarà tenuto ad accertare 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 il suddetto potrà visionare le immagini che lo riguardano.
3. La risposta alla richiesta di accesso a dati conservati deve essere inoltrata entro quindici giorni dalla ricezione e deve riguardare i dati attinenti alla persona richiedente e può comprenderne eventualmente altri, riferiti a terzi, solo nei limiti previsti dalla normativa vigente.
4. La Giunta Comunale quantificherà, mediante l'adozione di una propria deliberazione, un contributo spese da corrispondere da parte del richiedente a copertura dei costi sostenuti per l'espletamento della pratica qualora le riprese richieste comportassero la visione di periodi prolungati delle immagini.

CAPO IV
DISPOSIZIONI PARTICOLARI PER VARCHI DI ACCESSO, Z.T.L., APPARECCHIATURE MOBILI

Art. 22 – Controllo targhe varchi accesso strade della città

1. Il sistema di controllo dei varchi cittadini è finalizzato a controlli di sicurezza pubblica e acquisizione di dati esclusivamente per finalità di repressione e prevenzione dei reati.
2. L'accesso dei dati è appannaggio esclusivo delle forze di polizia e della magistratura.
3. La conservazione dei dati ha durata di 100 giorni oltre i quali il sistema cancella automaticamente le registrazioni

Art. 23 - Impianti controllo accessi zone traffico limitato

1. Gli impianti, qualora istallati, sono utilizzati per la rilevazione dei dati riguardanti il luogo, il tempo e l'identificazione dei veicoli che accedono al centro storico o nelle zone a traffico limitato. Gli impianti raccolgono dati sugli accessi rilevando immagini solamente in caso di infrazione alle norme del codice stradale.
2. La procedura sanzionatoria prevista dal titolo VI del codice della strada, ha luogo solamente in presenza di violazione documentata con immagini. A tal fine la custodia e l'utilizzazione dei dati rilevati dagli impianti sono riservati al responsabile dell'ufficio nel quale si elaborano i procedimenti sanzionatori per infrazioni al codice della strada ed al personale di polizia stradale. L'organo di polizia stradale, sulla base del rilevamento, accerta l'identità del soggetto destinatario della notifica della violazione e procede alla redazione del verbale di contestazione.
3. Al verbale non è allegata la documentazione con immagini che è custodita per eventuali contestazioni. La documentazione con immagini è utilizzata per le sole finalità di applicazione del procedimento sanzionatorio ed è conservata per il solo periodo necessario alla contestazione dell'infrazione, all'applicazione della sanzione ed alla definizione dell'eventuale contenzioso e comunque non oltre l'estinzione dell'obbligazione pecuniaria correlata all'infrazione.
4. Ferme restando le disposizioni di cui alla normativa *sulla privacy*, e successive modificazioni, i dati rilevati sono accessibili per fini di polizia giudiziaria o di indagine penale.
5. L'esercizio degli impianti ha luogo nel rispetto delle norme di omologazione od approvazione, per le finalità per cui sono stati autorizzati dal competente Ministero.
6. Gli impianti non sono interconnessi con altri strumenti, archivi o banche dati ad eccezione di quello che gestisce il contenzioso per violazioni al codice stradale, il gestionale per il rilascio delle autorizzazioni all'accesso alla zona a traffico limitato ed il gestionale per i procedimenti sanzionatori.
7. Gli impianti sono gestiti direttamente dall'organo di polizia stradale del Comune di Vittoria e sono nella disponibilità dello stesso. Durante il funzionamento degli impianti non è necessaria la presenza di un organo della polizia stradale ai fini dell'accertamento come previsto dal codice della strada.
8. L'accertamento delle violazioni rilevate, come previsto dall'articolo 385 del regolamento di attuazione del codice strada, può essere effettuato in tempo successivo con esonero della necessità di contestazione immediata.
9. I dati rilevati possono essere utilizzati anche per la riscossione del pagamento di eventuale tariffa stabilita per l'accesso all'area limitata al traffico ai sensi del codice della strada. Tale utilizzo è consentito solamente se il Comune si è avvalso della facoltà di subordinare al pagamento della tariffa l'ingresso o la circolazione dei veicoli a motore all'interno delle zone a traffico limitato, nel rispetto delle direttive a tal fine emanate dal competente Ministero.
10. Gli impianti di rilevazione possono essere altresì programmati per la rilevazione di dati necessari al recupero delle somme dovute in caso di mancato o insufficiente pagamento della tariffa.
11. I dati rilevati possono essere utilizzati, in forma anonima, nel rispetto delle vigenti disposizioni di legge, a fini statistici e per studi, analisi e rilievi di traffico.
12. Per quanto concerne la necessaria sicurezza delle operazioni di accesso, di riconoscimento o di trattamento automatico dei dati rilevati si rinvia alle disposizioni specifiche applicate per il sistema di videosorveglianza cittadina in quanto compatibili.
13. Il responsabile per la gestione e il trattamento dei dati rilevati con gli impianti di rilevazione di cui al presente articolo è il responsabile pro tempore dell'ufficio verbali/contenzioso del Corpo di Polizia Municipale.

Art. 24 - Utilizzo videoriprese con telecamere e fotocamere mobili o altra strumentazione video

1. Le apparecchiature di video sorveglianza mobili possono essere collocate nel rispetto delle norme del presente regolamento ed in particolare delle disposizioni sulla conservazioni delle immagini non eccedenti una settimana e le indicazioni di legge indicate negli appositi segnali collocati in zona.

2. In deroga all'obbligo della collocazione della segnaletica di riferimento eventuali videocamere possono essere posizionate per indagini di polizia giudiziaria, previo assenso della Magistratura.
3. Le immagini di riprese con telecamere da indossare (cosiddette body camera) sono soggette alle diposizione del presente regolamento, ad eccezione dell'obbligo di collocazione dei cartelli, e possono essere utilizzate solamente per la ricostruzioni di eventi con rilevanza penale. Tale immagini, in assenza di necessità di conservazioni ai fini di prova, vanno cancellate entro 24 ore dalla ripresa.
4. Le immagini riprese con palmari a fini sanzionatori possono essere mantenute sino alla definitiva conclusione del procedimento alle quali sono connesse e successivamente vanno cancellate.

Art. 25 - Utilizzo apparecchiature per rilievo mancata copertura assicurativa e altre violazioni al codice della strada

1. Le apparecchiature utilizzate per la rilevazione dei dati riguardanti il luogo, il tempo e l'identificazione dei veicoli che non hanno effettuato il pagamento della copertura assicurativa, la prescritta revisione o altri obblighi inerenti il codice stradale devono essere omologate ai sensi di legge.
2. I dati rilevati da queste apparecchiature possono essere utilizzati ai fini del procedimento sanzionatorio del codice stradale nonché per finalità di polizia giudiziaria (ricerca veicoli rubati, ecc.).

CAPO V
ILLECITI PENALI

Art. 26 – Accertamenti di illeciti ed indagini giudiziarie o di Polizia.

1. In caso di rilevazioni di immagini di fatti concernenti ipotesi di reato o di eventi rilevanti ai fini della pubblica sicurezza, della tutele ambientale o del patrimonio pubblico e privato, l'Incaricato o il Responsabile provvederà a darne comunicazione senza ritardo all'Autorità competente, provvedendo, nel contempo, alla conservazioni delle immagini su appositi supporti per l'utilizzo ai fini processuali sino alla conclusione del procedimento.
2. Alle immagini raccolte ai sensi del presente articolo possono accedere, per l'espletamento delle relative indagini, solo gli appartenenti all'Autorità Giudiziaria, le persone da essi espressamente autorizzate o delegate, e gli organi di Polizia.
3. Qualora gli organi di Polizia, nello svolgimento dei loro compiti istituzionali, necessitino di una copia delle riprese effettuate, devono presentare un'istanza scritta e motivata indirizzata al Responsabile del trattamento dei dati.
4. I privati cittadini possono fare istanza di salvataggio delle immagini, nelle more dell'attivazione dei procedimenti giudiziari, entro il termine di cancellazione stabilito nel regolamento. Le immagini salvate resteranno a disposizione esclusivamente delle forze di Polizia Giudiziaria e della Magistratura ai fini dell'accertamento dei fatti.

CAPO VI
MISURE DI SICUREZZA

Art. 27 – Misure di sicurezza - Sistemi di autenticazione informatica

1. E' obbligatorio che l'accesso alle immagini e ai dati connessi (anche sotto forma di estrazione, manipolazione, cancellazione, ecc.) avvenga solo attraverso credenziali di autenticazione che consentano il superamento di una procedura di autenticazione, fatta eccezione della visione dei monitor collegati direttamente alle telecamere analogiche o a semplici uscite di segnali video dai videoregistratori, a meno che le apparecchiature dalle quali originano le sorgenti non siano in grado di gestire automaticamente l'autenticazione informatica.
2. Le credenziali di autenticazione devono consistere, per ciascuna utenza, in un codice per l'identificazione dell'incaricato (usseri) associato a:
   - una parola chiave (password) riservata e differente dalle altre, oppure ad un dispositivo di autenticazione con credenziali uniche, eventualmente associato a un codice identificativo (usseri) oltre che alla password;

- un'eventuale caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave;
- la parola chiave (password), quando è prevista, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. E' consigliabile, ma non obbligatorio, che il sistema sia in grado di controllare, informatica mente e in forma sicura, che la parola chiave non contenga riferimenti agevolmente riconducibili all'incaricato, sia modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi e qualora si verifichi il trattamento di dati sensibili e/o di dati giudiziari sia modificata almeno ogni tre mesi.

Art. 28 – Misure di sicurezza - Sistemi di controllo del sistema informatico

1. Il sistema informatico, oppure tramite indirizzi organizzativi forniti dal Titolare o dal Responsabile del Trattamento, deve essere in grado di controllare, informaticamente e in forma sicura, che il codice per l'identificazione (usseri) non possa essere assegnato ad altri incaricati, neppure in tempi diversi e che le credenziali di autenticazione non utilizzate da almeno sei mesi siano disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
2. E' obbligatorio, che il sistema di videosorveglianza supporti sistemi di accesso dei profili basati su autorizzazione differenti (ad es. solo visione, visione registrato e gestione preste, amministratori) e che tutti gli incaricati debbano essere automaticamente associati ai profili supportati.

Art. 29 – Misure di sicurezza - Altre misure di sicurezza

1. E' obbligatorio che il sistema di videosorveglianza sia protetto (mediante l'attivazione di idonei strumenti elettronici) contro il rischio di intrusione e dell'azione di programmi idonei a danneggiarlo, ivi comprese le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero sia protetto da programmi in grado di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Per tale motivo deve essere dotato di sistema antivirus aggiornato e funzionante gestito dal competente ufficio informatico. Il sistema deve effettuare automaticamente l'aggiornamento con cadenza periodica ravvicinata dei programmi (comunque per periodi non superiore a sei mesi) volti a prevenire la vulnerabilità degli strumenti elettronici (ad es.: aggiornamento e installazione di patch sui sistemi operativi).
2. E' comunque obbligatorio che anche gli apparati da ripresa digitali che trattano dati sensibili o giudiziari, ovvero i cui sistemi siano connessi in rete, siano protetti (mediante l'attivazione di idonei strumenti elettronici) contro l'accesso abusivo dall'esterno.
3. I supporti rimovibili contenenti dati sensibili o giudiziari, se non utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
4. Le immagini salvate su supporti rimovibili o con telecamere mobili vanno conservate in luogo inaccessibile, chiuso e protetto a cura del responsabile del trattamento e degli incaricati dello stesso.
5. E' obbligatorio che il Responsabile della gestione tecnica adotti le misure idonee affinché la trasmissione tramite la rete pubblica di comunicazioni delle immagini riprese dagli apparati sia effettuata previa applicazione di sistemi che ne garantisca la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless.

Art. 30 – Misure di sicurezza - misure di autenticazione per soggetti terzi

1. E' consigliabile, ma non obbligatorio, che per gli utenti dotati di credenziali di autenticazione per effettuare la manutenzione degli impianti sia comunque prevista una doppia chiave logica per la visione delle immagini, in maniera che il consenso alla visione delle stesse possa essere dato solo da un utente dotato di poteri di semplice visione delle stesse; qualora non sia tecnicamente possibile implementare questa misura con strumenti elettronici, essa può essere adottata con strumenti organizzativi, in maniera che l'accesso venga garantito solo se ciò si renda indispensabile al fine di effettuare le eventuali verifiche tecniche.

Art. 31 – Misure di sicurezza - misure in caso di sistemi integrati gestiti da privati o da altri soggetti pubblici

1. Qualora il sistema di videosorveglianza sia collegato con soggetti privati che abbiano possibilità di visione o accesso al sistema deve essere prevista la registrazione degli accessi logici dei citati oggetti privati e le loro operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con capacità di conservazione per un periodo di tempo comunque non inferiore a sei mesi.
2. Altresì è obbligatorio che in caso di utilizzo di sistemi integrati di videosorveglianza gli stessi debbano consentire la separazione logica delle immagini registrate dai diversi soggetti distinguendo tra quelli pubblici e quelli privati.
3. E' obbligatorio che in caso di utilizzo di sistemi integrati di videosorveglianza da parte di vari soggetti pubblici, l'utilizzo condiviso, in forma integrale o parziale, di detti sistemi, tramite la medesima infrastruttura tecnologica, debba essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando di tracciare gli spostamenti degli interessati (quindi delle persone riprese) e di ricostruirne il percorso effettuato in aree o attività che esulano dalla competenza istituzionale dell'ente; a tal scopo è obbligatorio che i contitolari del trattamento predispongano idonee misure atte a garantire che i dati personali raccolti siano trattati in forma differenziata e rigorosamente distinta, in relazione alle competenze istituzionali della singola pubblica amministrazione.
4. E' obbligatorio che, in caso di utilizzo di sistemi di videosorveglianza soggetto alla normativa sull'Amministratore di sistema, debbano essere adottati, a cura del responsabile della gestione tecnica del sistema, idonei accorgimenti che prevedano la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione agli archivi elettronici da parte di tutti i soggetti interessati. Le registrazioni (accesso log) debbono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate un periodo di tempo comunque non inferiore a sei mesi o una capacità di conservazione maggiore, in quanto il titolare del trattamento deve valutare il periodo congruo all'esercizio dei doveri di verifica periodica dell'operato degli amministratori di sistema.

Art. 32 – Sicurezza dei dati

1. I dati sono protetti da idonee e preventive misure di sicurezza, individuate con documentazione tecnica rilasciata dalla ditta installatrice del software, riducendo al minimo i rischi di distruzione, di perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
2. Il Responsabile della gestione tecnica deve provvedere all'implementazione e aggiornamento costante delle misure idonee a garantire la sicurezza dei dati.
3. Vanno comunque assicurate alcune misure, cosiddette minime, obbligatorie anche dal punto di vista penalistico, ed in particolare accessi differenziati tra i vari operatori, inaccessibilità alla sala server ubicata presso la sede del Comune, sovrascrittura delle immagini decorsi i tempi di legge.
4. I dati personali oggetto di trattamento giudiziario o sensibile sono custoditi nella centrale di visione situata presso la sede della Polizia Municipale in formato informatico e/o cartaceo qualora debbano essere utilizzati a fini di prova per attività di polizia giudiziaria. In tale ufficio, ubicato all'interno del Comando, possono accedere esclusivamente il Responsabile e gli incaricati del trattamento dei dati. Non possono accedervi altre persone se non sono accompagnate da soggetti autorizzati.

Art. 33 – Modalità da adottare per i dati video ripresi

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; a tal scopo l'accesso alla sala di videosorveglianza è chiusa e viene interdetta a chiunque non sia incaricato durante la trasmissione delle immagine sui monitor. La visione di immagini riprese con videocamere mobili deve avvenire in ufficio inaccessibile al momento della visione delle stesse e il salvataggio delle immagini, limitato per l'espletamento degli iter sanzionatori, effettuato su computer per i quali gli accessi avvengono con password. Le immagini o fotogrammi non utilizzabili a fini sanzionatori vanno immediatamente e definitivamente cancellati. Le immagini riprese ai sensi del capo IV del presente regolamento ed inerenti le modalità di accertamenti ingressi in c.t. oppure finalizzate agli accertamenti di violazioni al codice stradale o altri illeciti amministrativi devono avvenire senza la presenza di soggetti non autorizzati e conservate nel gestionale del contenzioso oppure nell'ufficio che gestisce l'illecito accertato.

2. L'accesso alle immagini da parte del Responsabile e degli incaricati 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 e sono soggette a segreto d'ufficio.
3. Nel caso le immagini siano conservate su supporti portatili, i relativi supporti vengono custoditi, per l'intera durata della conservazione, in un armadio o simile struttura dotato di serratura, apribile solo dal Responsabile e dagli incaricati del trattamento dei dati.
4. La cancellazione delle immagini sarà garantita mediante gli strumenti e le procedure tecnologiche più avanzate; le operazioni di cancellazione devono essere effettuate esclusivamente sul luogo di lavoro.
5. Nel caso il supporto debba essere sostituito per eccessiva usura, sarà distrutto in modo da renderlo inutilizzabile, in modo che non possano essere recuperati i dati in esso presenti.
6. L'accesso alle immagini ed ai dati personali è consentito:
   a) al Responsabile ed agli incaricati dello specifico trattamento di cui al presente regolamento;
   b) ai preposti alle indagini delegati dall'Autorità Giudiziaria o di polizia giudiziaria previa identificazione su apposito registro;
   c) all'Amministratore di Sistema del Comune di Vittoria e alla ditta fornitrice dell'impianto nei limiti strettamente necessari alle loro specifiche funzioni di manutenzione sempre previa identificazione e registrazione e nel rispetto delle disposizioni del presente regolamento;
   d) all'interessato, debitamente autorizzato, in quanto oggetto delle riprese, salvo i diritti dei controinteressati.
7. Nel caso di accesso ai dati da parte dell'interessato questi avrà visione solo delle immagini che lo riguardano direttamente.
8. Tutti gli accessi alla visione saranno documentati mediante l'annotazione in un apposite "registro degli accessi" (cartaceo od informatico), conservato nei locali della centrale operativa della Polizia Municipale, nel quale sono riportati ad opera degli incaricati:
a) la data e l'ora dell'accesso;
b) l'identificazione del terzo autorizzato;
c) i dati per i quali si è svolto l'accesso;
d) gli estremi e la motivazione dell'autorizzazione all'accesso;
e) le eventuali osservazioni dell'incaricato;
   la sottoscrizione del medesimo.

Art. 34 – Cessazione dell'attività di videosorveglianza

1. In caso di cessazione, per qualsiasi causa, dell'attività di videosorveglianza, il Comune di Vittoria effettuerà la notificazione al Garante e ed in quanto dovuta ai sensi della vigente normativa.
2. A seguito di ciò i dati raccolti dovranno essere distrutti o conservati per fini esclusivamente istituzionali.
3. La cessione dei dati in violazione al comma precedente è da considerarsi priva di effetti e sono fatte salve le sanzioni previste dalla Legge.

Art. 35 – Comunicazione dei dati

1. La comunicazione dei dati personali acquisiti mediante il sistema di videosorveglianza, da parte del Comune di Vittoria, avviene solamente a soggetti pubblici autorizzati ed è ammessa quando necessaria ed esclusivamente per lo svolgimento delle funzioni istituzionali. E' escluso il rilascio di immagini a soggetti privati e consentito solo se previsto da norme di legge e regolamenti.
2. Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, la conoscenza dei dati personali da parte delle persone incaricate ed autorizzate per iscritto a compiere le operazioni del trattamento dal titolare o dal Responsabile e che operano sotto la loro diretta autorità.
3. E' in ogni caso fatta salva la comunicazione 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'articolo 58, comma 2, del D.lgs. 30/6/2003 n. 196 per finalità di difesa di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati e tale attività viene disciplinata dalle espresse disposizioni di legge nonché quelle di cui agli articoli 23 e 24 del decreto legislativo 18 maggio 2018, n. 51.
4. Non possono essere rilasciate copie delle immagini registrate dal sistema di videosorveglianza se non per finalità di giustizia e ai soggetti indicati nel presente regolamento e/o esclusivamente secondo diposizioni di

legge. Le immagini registrate per finalità di accertamento di illeciti stradali o amministrativi possono essere rilasciate secondo le procedure stabilite per l'acceso agli atti e previo pagamento dei relativi costi.

Art. 36 – Valutazione di impatto sulla protezione dei dati

1. Per quanto non previsto dal presente regolamento si rinvia alla valutazione di impatto sulla privacy ossia alla procedura finalizzata alla redazione di apposito documento volto a descrivere il trattamento, valutarne l'effettiva necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali (attraverso quindi la valutazione di tali rischi e la definizione delle misure idonee ad affrontarli da redigere nel D.P.I.A. "*Data Protection Impact Assessment"* previsto nel regolamento europeo UE n. 2016/679).

CAPO VII
NORME FINALI

Art. 37 – Norma di rinvio

1. Per tutto quanto non disciplinato dal presente Regolamento si fa rinvio alle Leggi vigenti ed in particolare al regolamento UE n. 2016/679 e al Decreto Legislativo 18 maggio 2018 n° 51 di attuazione della direttiva (UE) 2016/680 del parlamento europeo e del consiglio del 27 aprile 2016 per quanto concerne il trattamento dei dati da parte di autorità a fini di prevenzione, indagine, accertamento e perseguimento dei reati, ai provvedimenti attuativi delle medesime, alle decisioni del Garante e ad ogni altra normativa, speciale, generale, nazionale e comunitaria in materia di protezione e trattamento dei dati personali nell'ambito della videosorveglianza.

Art. 38– Tutela amministrativa e giurisdizionale

1. La mancata osservanza degli obblighi previsti dal presente Regolamento comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla Legge, di sanzioni amministrative o penali.
2. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale, si rinvia integralmente alle disposizioni contenute nelle leggi vigenti.
3. Il responsabile del procedimento, ai sensi e per gli effetti della legge 7 agosto 1990, n. 241 è il responsabile del trattamento dei dati personali e gli incaricati al trattamento, come indicati nel presente regolamento; in particolare, per la gestione dei dati afferenti alle violazioni del codice stradale o all'accertamento di illeciti amministrativi, sono responsabili dei procedimenti gli accertatori e, per la parte specifica di trattamento dei dati. Gli incaricati degli uffici e/o il responsabile pro tempore dell'ufficio contenzioso.

Art. 39 – Modifiche regolamentari

1. I contenuti del presente Regolamento dovranno essere aggiornati nei casi di variazioni delle normative in materia di trattamento dei dati personali, gerarchicamente superiori.
2. Il presente atto è trasmesso al Garante per la protezione dei dati personali, sia a seguito della sua approvazione, sia in caso di eventuali successivi aggiornamenti.
3. Il presente Regolamento entrerà in vigore con le modalità ed i tempi stabiliti dallo Statuto Comunale.
4. L'ubicazione delle telecamere del sistema di videosorveglianza viene indicata ed aggiornata con apposita determinazione dirigenziale ed indicata con i prescritti cartelli come previsto nel presente regolamento.
5. L' installazione di telecamere mobili per la videosorveglianza ambientale e per le finalità di cui all'art. 4 comma 2 let. B del presente regolamento, avverrà su siti individuati dal Comando di Polizia Municipale.

Art. 40 – Limiti alla utilizzabilità di dati personali

1. La materia è disciplinata oltre che dal citato regolamento europeo anche dal "Codice in materia di protezione dei dati personali" approvato con decreto legislativo 30 giugno 2003 n. 196, integrato con le modifiche introdotte dal D. Lgs 101/2018.

Art. 41 – Danni cagionati per effetto del trattamento di dati personali

1. La materia è regolamentata per l'intero dalla normativa vigente. I soggetti incaricati del trattamento dei dati sono obbligati per legge alla segretezza e riservatezza.