



COMUNE di FORGARIA NEL FRIULI
Provincia di Udine



REGOLAMENTO COMUNALE
PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA

Approvato con deliberazione del Consiglio Comunale n. _____ del _____

INDICE

CAPO I

- PRINCIPI GENERALI

- Articolo **1** - **Finalità e definizioni**
- Articolo **2** - Ambito di applicazione
- Articolo **3** - Trattamento dati personali - Finalità istituzionali dell'impianto di videosorveglianza

CAPO II

- OBBLIGHI PER IL TITOLARE DEL TRATTAMENTO

- Articolo **4** - Notificazione
- Articolo **5** - Responsabile

CAPO III

- TRATTAMENTO DEI DATI PERSONALI

Sezione I - RACCOLTA E REQUISITI DEI DATI PERSONALI

- Articolo **6** - Modalità di raccolta e requisiti dei dati personali
- Articolo **7** - Obblighi degli operatori
- Articolo **8** - Accertamenti di illeciti e indagini di Autorità Giudiziarie o di Polizia
- Articolo **9** - Informazioni rese al momento della raccolta

Sezione II - DIRITTI DELL'INTERESSATO NEL TRATTAMENTO DEI DATI

- Articolo **10** - Diritti dell'interessato
- Articolo **11** - Sistemi integrati di videosorveglianza
- Articolo **12** - Ulteriori avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici ovvero da enti territoriali.-

Sezione III - SICUREZZA NEL TRATTAMENTO DEI DATI, LIMITI ALLA UTILIZZABILITA' DEI DATI E RISARCIMENTO DEI DANNI

- Articolo **13** - Sicurezza dei dati
- Articolo **14** - Istituti scolastici
- Articolo **15** - Il deposito dei rifiuti
- Articolo **16** - Cessazione del trattamento dei dati
- Articolo **17** - Limiti alla utilizzabilità di dati personali
- Articolo **18** - Danni cagionati per effetto del trattamento di dati personali

Sezione IV - COMUNICAZIONE E DIFFUSIONE DEI DATI

- Articolo **19** - Comunicazione

CAPO IV

- TUTELA AMMINISTRATIVA E GIURISDIZIONALE

- Articolo **20** - Tutela

CAPO V

- MODIFICHE

- Articolo **21** - Modifiche regolamentari

A seguire fac-simili di moduli e domande.

CAPO I

PRINCIPI GENERALI

Articolo 1

FINALITÀ E DEFINIZIONI

1) Il presente regolamento disciplina l'esercizio e l'organizzazione degli impianti e del servizio di videosorveglianza gestito dal Comune di Forgaria nel Friuli, ne regola l'uso nei limiti imposti dal D. lgs. 30.06.2003, n. 196 "Codice in materia di protezione dei dati personali" e ne determina le condizioni necessarie affinché gli impianti possano essere tenuti in esercizio, nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.-

2) L'uso di impianti di videosorveglianza è finalizzato alla prevenzione e repressione degli atti delittuosi, delle attività illecite e degli episodi di microcriminalità che, perpetrati sul territorio comunale, ivi compresi gli immobili di proprietà o in gestione all'Amministrazione, possono determinare danno ai cittadini, ai beni di proprietà od in gestione all'Amministrazione comunale.

Il sistema è di ausilio alle forze di Polizia Locale nell'azione di tutela e di controllo del territorio. Tali impianti possono essere altresì utilizzati per il monitoraggio del traffico cittadino in modo da rappresentare un valido strumento per l'intervento tempestivo della stessa Polizia Locale nelle situazioni di rischio o di pericolo.-

L'attività di videosorveglianza si colloca nella cornice normativa relativa allo svolgimento delle funzioni istituzionali e non è pertanto finalizzata alla raccolta e al trattamento di dati sensibili. Non è escluso che la registrazione di particolari comportamenti possa far risalire ad informazioni identificate a termini di legge.

3) La responsabilità della gestione dell' impianto, il suo costante adeguamento alle norme di sicurezza previste dalla normativa e il costante controllo sull'uso delle immagini inquadrare e raccolte, spetta al responsabile del trattamento dati della videosorveglianza.

Il responsabile del trattamento dati della videosorveglianza viene individuato nel Responsabile del Servizio di Polizia Locale. Tale figura, che sarà da ora denominata "responsabile dell'impianto", potrà individuare gli incaricati del trattamento, di cui all'articolo 30 del D. lgs. 196/2003.

Il responsabile e gli eventuali incaricati procederanno al trattamento dati attenendosi alle istruzioni ricevute dal titolare (**Comune**) il quale, attraverso periodiche verifiche, vigilerà sulla puntuale esecuzione delle procedure stabilite dal presente regolamento.

4) Le immagini raccolte dalle telecamere (**dati personali**) oggetto di trattamento saranno:

- a) trattate in modo lecito e secondo correttezza;
- b) raccolte e registrate esclusivamente per le finalità di cui al comma 2) dell'art. 1 del presente regolamento;
- c) raccolte in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolte o successivamente trattate;
- d) conservate per un periodo di tempo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, per le quali esse sono state raccolte o successivamente trattate.-

Le immagini raccolte non potranno assolutamente essere utilizzate per finalità diverse da quelle stabilite al comma 2) dell'art. 1 del presente regolamento ed in particolare secondo quanto segue:

- a) gli impianti di videosorveglianza non potranno essere utilizzati, in base all'articolo 4 dello Statuto dei Lavoratori (*legge 20 maggio 1970, n. 300*), per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati;
- b) gli impianti di videosorveglianza non potranno essere utilizzati per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati o per finalità di promozione turistica;

- c) i dati acquisiti della circolazione stradale non potranno essere collegati con altre banche dati .-

5) I dati raccolti tramite i sistemi di videosorveglianza sono da considerarsi "dati sensibili" ai sensi del D. Lgs. 196/2003 e dovranno quindi essere trattati secondo quanto previsto nel citato decreto. L'accesso ai dati potrà avvenire solamente da parte degli organi della Pubblica Amministrazione per l'espletamento dei propri fini istituzionali inerenti la giustizia, l'attività di polizia e tutela dei beni.

I dati raccolti non potranno in alcun modo essere spediti alla residenza o domicilio delle persone eventualmente sanzionate.

La custodia dei dati dovrà avvenire in armadi di sicurezza chiusi a chiave e solo il responsabile dell'impianto o suo delegato potrà accedervi.

6) La presenza dell' impianto di videosorveglianza sarà resa pubblica, a cura del responsabile dell'impianto, attraverso i mezzi ritenuti più idonei ed in particolare attraverso:

- a) l'affissione di appositi cartelli posizionati nei punti del comune ove sono presenti le telecamere recanti la scritta tipo "Videosorveglianza in funzione" – "area videosorvegliata" – od altra dicitura facilmente leggibile";
- b) verrà reso pubblico all'Albo c.le, il nominativo del "responsabile dell'impianto" di cui al comma 3 dell'art. 1 del presente regolamento; unitamente all'elenco delle posizioni delle telecamere;
- c) Copia del presente regolamento verrà trasmesso alle diverse Autorità di Polizia statali e/o regionali.

7) Le inquadrature dovranno essere tali da cogliere un'immagine panoramica delle persone e dei luoghi, evitando riprese inutilmente particolareggiate tali da essere eccessivamente intrusive della riservatezza delle persone ove ciò non sia funzionale alle finalità istituzionali del sistema, garantendo comunque la possibilità di identificazione dei responsabili degli illeciti ove necessario.-

- a) L'uso dell'immagine particolareggiata è consentito esclusivamente quale supporto logistico ad operazioni di polizia o finalizzato all'accertamento di infrazione alla legge.-
- b) Le immagini provenienti dalle telecamere saranno raccolte in una stazione di monitoraggio e controllo presso la centrale operativa della Polizia Locale. In questa sede le immagini saranno registrate su disco fisso del computer, onde consentire la ricostruzione di eventi, anche in assenza di presidio della stazione di monitoraggio.-

8) Le registrazioni dovranno essere conservate per un massimo di **7 giorni**, trascorsi i quali, le immagini nuove prenderanno il posto delle vecchie. Qualora pervenga copia di denuncia di reato, le sole immagini utili alla ricerca dei responsabili degli atti saranno riversate su un nuovo supporto al fine della loro conservazione in relazione agli illeciti o alle indagini delle autorità giudiziarie o di polizia. I supporti utilizzati per la memorizzazione delle immagini, al termine del loro periodo di utilizzo conveniente, saranno distrutti previa cancellazione delle immagini registrate.-

9) Per tutto quanto non è dettagliatamente disciplinato nel presente regolamento, si rinvia a quanto disposto dal **Codice** in materia di **protezione dei dati personali**, approvato con **Decreto Legislativo 30 giugno 2003, n. 196** e s.m.i. ed al **provvedimento del Garante, dd. 8 aprile 2010 (10A05072)** in materia di videosorveglianza pubblicato in **Gazzetta Ufficiale nr. 99 del 29/04/2010** e s.m.i. .-

10) per quanto innanzi detto, si stabilisce che la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini, configurano un trattamento di dati personali, ove:

- a) per "**banca di dati**", *si intende*, il complesso di dati personali, formatosi presso la sala di controllo, è trattato esclusivamente mediante riprese televisive che, in relazione ai luoghi di installazione delle videocamere, riguardano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto;

- b) per il "**trattamento**", *si intende*, tutte le operazioni o complesso di operazioni, svolte con l'ausilio dei 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, l'eventuale diffusione, la cancellazione e la distribuzione di dati;
- c) per "**dato personale**", *si intende*, qualunque informazione relativa a persona fisica, persona giuridica, Ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione e rilevati con trattamenti di immagini effettuati attraverso l'impianto di videosorveglianza;
- d) per "**titolare**", *si intende*, l'Ente Comune di Forgaria nel Friuli, nelle sue articolazioni interne, cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali;
- e) per "**responsabile**", *si intende*, la persona fisica, legata da rapporto di servizio al titolare e preposto dal medesimo al trattamento dei dati personali;
- f) per "**interessato**", *si intende*, la persona fisica, la persona giuridica, l'Ente o associazione cui si riferiscono i dati personali;
- g) per "**comunicazione**", *si intende*, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- h) per "**diffusione**", *si intende*, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- i) per "**dato anonimo**", *si intende*, il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- j) per "**blocco**", *si intende*, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.
- k) per "**brandeggio**", *si intende*, il supporto della videocamera che ruota sull'asse verticale e su quello orizzontale, comandato a distanza dalla consolle centrale.

Articolo 2

AMBITO DI APPLICAZIONE

- 1) Il presente regolamento disciplina il trattamento di dati personali, realizzato mediante l'impianto della videosorveglianza, attivato nel territorio urbano del Comune di Forgaria nel Friuli, collegato alla sala di controllo attivata in appositi locali municipali di competenza della polizia locale.-
- 2) Tutti i dati rilevati dalle stazioni fisse di videosorveglianza verranno inviati, attraverso una rete regionale protetta, alla "sala operativa" presso la sede di "**Protezione Civile**" di Palmanova.-
- 3) Potenzialmente, potrà essere valutata l'opportunità di collegarsi, per la sola visione delle immagini, alle centrali operative del Comando Carabinieri e del Commissariato, di Tolmezzo.-
- 4) L'utilizzo dei sistemi di videosorveglianza viene attuato attraverso un corretto impiego delle applicazioni e nel rispetto dei principi di:
 - **liceità**, quale rispetto della normativa sia per gli organi pubblici che privati;
 - **proporzionalità**, con sistemi attuati con attenta valutazione;
 - **finalità**, attuando il trattamento dei dati solo per scopi determinati ed espliciti;
 - **necessità**, con esclusione di uso superfluo della videosorveglianza.-

Articolo 3

TRATTAMENTO DATI PERSONALI FINALITÀ ISTITUZIONALI IMPIANTO DI VIDEOSORVEGLIANZA

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

2) Le finalità istituzionali del suddetto impianto, sono del tutto conformi alle funzioni istituzionali demandate al Comune di Forgaria nel Friuli, dal D.L.vo 18 agosto 2000, n. 267, dal D.P.R. 24 luglio 1977, n.616, dalla legge sull'ordinamento della Polizia Locale 7 marzo 1986, n. 65, dalla Legge Regionale del 14.04.2003, n. 3, nonché dallo Statuto Comunale, dai Regolamenti Comunali vigenti e dalla legge 24.07.2008, n. 125, recante "**Misure urgenti in materia di sicurezza urbana**". *che ha novellato* l'art. 54 del d.lgs. 267/200; e loro ss.mm.ii., ed in particolare:

- a) attivare uno strumento attivo di sicurezza urbana e/o di protezione civile sul territorio comunale.-
- b) identificare, anche in tempo reale, luoghi o aree pubbliche, giudicate sensibili, anche per un pronto intervento.-
- c) monitorare, anche in remoto, al fine di accrescere la sicurezza urbana, eventuali atti, *esempio*:
 - vandalismo o danneggiamento agli immobili ed in particolare al patrimonio comunale pubblico;
 - disturbo alla quiete pubblica;
 - sicurezza pubblica - incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, quali: l'ordine, la prevenzione, l'accertamento e/o repressione dei reati svolti da soggetti diversi verso il patrimonio pubblico, a valenza pubblica e/o privato, ovvero verso le persone.-
- d) proteggere/salvaguardare la proprietà pubblica o di interesse pubblico.-
- e) rilevare, prevenire, controllare, anche in remoto, e se del caso, il traffico stradale ai fini di indagini, ovvero anche per migliorare la fruibilità e sicurezza delle strade, piazze o aree pubbliche (*es. controllo parcheggi pubblici in generale*).-
- f) acquisire prove a valenza civile e/o penale, a seguito di fatti od atti penalmente/civilmente rilevanti.-

3) 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 ed i mezzi di trasporto che si troveranno ad operare/transitare nelle aree rientranti nel raggio di azione delle videocamere.-

CAPO II

OBBLIGHI PER IL TITOLARE DEL TRATTAMENTO

Articolo 4

NOTIFICAZIONE

Il Comune di Forgaria nel Friuli nella sua qualità di titolare del trattamento dei dati personali, rientrante nel campo di applicazione del presente regolamento, adempie agli obblighi di notificazione preventiva al Garante per la protezione dei dati personali, qualora ne ricorrano i presupposti, ai sensi e per gli effetti degli artt. 37 e 38 del **Codice** in materia di protezione dei dati personali approvato con **Decreto Legislativo 30/6/2003, n. 196** e s.m.i. -

Articolo 5

RESPONSABILE

1) Il Responsabile del Servizio di Polizia locale del Comune di Forgaria nel Friuli è designato quale Responsabile del trattamento dei dati personali rilevati, ai sensi per gli effetti dell'art. 1, *comma 3, lett. e*).- E' consentito il ricorso alla **delega** scritta di funzioni da parte del predetto Responsabile, previa approvazione/visto del Sindaco.-

2) Il Responsabile (*ovvero l'incaricato con delega scritta*) deve rispettare pienamente quanto previsto, in tema di trattamento dei dati personali, dalle leggi vigenti, ivi incluso il profilo della sicurezza, e dalle disposizioni del presente Regolamento.-

3) Il Responsabile procede al trattamento attenendosi alle istruzioni impartite dal titolare di posizione (*Responsabile del servizio di Polizia locale*), il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al *comma 2*) e delle proprie istruzioni.-

4) I compiti affidati al **Delegato** devono essere analiticamente specificati per iscritto, in sede di designazione. Gli **incaricati** devono elaborare i dati personali, ai quali hanno accesso, attenendosi scrupolosamente alle istruzioni impartite del titolare/responsabile.-

CAPO III

TRATTAMENTO DEI DATI PERSONALI

Sezione I

RACCOLTA E REQUISITI DEI DATI PERSONALI

Articolo 6

MODALITÀ DI RACCOLTA E REQUISITI DEI DATI PERSONALI

1) I dati personali oggetto di trattamento sono:

- a) trattati in modo lecito e secondo correttezza;
- b) raccolti e registrati per le finalità di cui al precedente art. **3** e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi, esatti e, se necessario, aggiornati;
- c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- d) conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, per le quali essi sono stati raccolti o successivamente trattati ed in ogni caso pari al periodo di tempo stabilito dal successivo *comma 4*);
- e) trattati, con riferimento alla finalità dell'analisi dei flussi del traffico, di cui al precedente art. *3 comma 2, lett. e)* ed *f)*, con modalità volta a salvaguardare l'anonimato ed in ogni caso successivamente alla fase della raccolta, atteso che le immagini registrate possono contenere dati di carattere personale.-

2) I dati personali sono ripresi attraverso le telecamere dell'impianto di telecontrollo e videosorveglianza, installate in corrispondenza di intersezioni, piazze, parchi pubblici e immobili, del territorio urbano, in conformità all'elenco dei siti di ripresa, adottato dall'Amministrazione Comunale con apposito atto **Giuntale**. Detta procedura verrà seguita anche in caso di modifiche e/o integrazioni delle postazioni.-

3) Le telecamere di cui al precedente *comma 2* consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario. Inoltre alcune telecamere potranno essere dotate di brandeggio e di zoom ottico e digitale e se del caso, anche dotate di infrarosso, collegate ad un centro di gestione ed archiviazione di tipo digitale.- Tali caratteristiche tecniche consentono un significativo grado di precisione e di dettaglio della ripresa. Il titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto attivato di cui al suddetto art. **3**. I segnali video delle unità di ripresa saranno raccolti da una stazione di monitoraggio e controllo presso la sala controllo dell'ufficio di Polizia Locale. In questa sede le immagini saranno visualizzate su monitor e registrate su un supporto magnetico. L'impiego del sistema di videoregistrazione è necessario per ricostruire l'evento, quando la sala di controllo non è presidiata.-

4) Le attività di videosorveglianza sono finalizzate alla tutela della sicurezza urbana. A luce delle recenti disposizioni del **Garante**, il termine massimo di durata della conservazione dei dati delle immagini raccolti/registrati è limitato ai **sette giorni**, fatte salve **speciali** esigenze di ulteriore conservazione.- In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla **settimana**, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del **Garante**, e comunque essere ipotizzata dal **titolare/responsabile** come eccezionale nel rispetto del principio di **proporzionalità**.- La congruità di un termine di tempo più ampio di conservazione va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità.- La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'**Autorità giudiziaria** o dalla **Polizia giudiziaria** in relazione ad un'attività investigativa in corso.-

Il sistema impiegato dovrà 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. *In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di expiring/cancellazione dei dati registrati, cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni alla fine del periodo di conservazione fissato dal titolare/responsabile dovrà 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.*

Articolo 7

OBBLIGHI DEGLI OPERATORI

1) L'utilizzo del brandeggio da parte degli operatori e degli incaricati al trattamento dovrà essere conforme ai limiti indicati dalla legge e nel rispetto del precedente articolo **6**).-

2) L'utilizzo delle telecamere è consentito solo per il controllo di quanto si svolga nei luoghi pubblici mentre esso non è ammesso nelle proprietà private.-

- Fatte salve le possibilità di stipulare apposite convenzioni, nel rispetto della legge, con Enti regionali, provinciali, religiosi, scolastici, ecc. - senza finalità lucrative o di mero interesse economico-privatistico, che abbiano attivato od in essere un sistema di videosorveglianza convergente con l'interesse primario pubblico generale.-

3) I soggetti "**privati**", motivatamente interessati, possono presentare istanza per la verifica dei dati registrati, questi ultimi possono essere riesaminati; *nel limite del tempo ammesso per la conservazione di cui al precedente articolo **6*** ; solo in caso di effettiva necessità e per il conseguimento delle finalità di cui all'art. 3, sempre comunque a seguito di regolare autorizzazione da parte del Responsabile della Polizia locale, titolare del trattamento dei dati personali registrati.-

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.-

Articolo 8

ACCERTAMENTI DI ILLECITI E INDAGINI DI AUTORITA' GIUDIZIARIE O DI POLIZIA

Ove dovessero essere rilevate immagini di fatti identificativi di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica, della tutela ambientale o del patrimonio, l'Incaricato/delegato provvederà ad informare il Responsabile della Polizia locale, il quale a sua volta, provvederà a darne immediata comunicazione agli organi competenti.-

In tali casi, in deroga alla puntuale prescrizione delle modalità di ripresa di cui al precedente articolo 7, l'incaricato, su mandato del Responsabile, procederà alla registrazione delle stesse su supporti magnetici.-

Alle informazioni raccolte ai sensi del presente articolo possono accedere solo gli organi di Polizia e l'Autorità Giudiziaria.-

L'apparato di videosorveglianza potrà essere utilizzato anche in relazione ad indagini disposte dall'Autorità Giudiziaria, di organi di Polizia o di Polizia Locale.-

Nel caso in cui gli organi di Polizia, nello svolgimento di loro indagini, necessitino di avere informazioni ad esse collegate che sono contenute nelle riprese effettuate, possono farne richiesta scritta e motivata indirizzandola al Responsabile della Polizia locale Titolare della gestione e del trattamento dei dati.

Articolo 9

INFORMAZIONI RESE AL MOMENTO DELLA RACCOLTA

1) Il Comune di Forgaria nel Friuli in ottemperanza a quanto disposto dall'art. 13 del Decreto Legislativo 30/6/2003 n. 196 e s.m.i.. ed al **provvedimento** del **Garante**, dd. **8 aprile 2010 (10A05072)** in materia di **videosorveglianza** pubblicato in **Gazzetta Ufficiale nr. 99 del 29/04/2010** e s.m.i., si obbliga ad affiggere un'adeguata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere, su cui va riportata la seguente dicitura: **Area videosorvegliata – La registrazione è effettuata dal Comando di Polizia Locale per fini di sicurezza urbana** come indicato nel successivo *comma.3*.

2) Il Comune di Forgaria nel Friuli nella persona del Responsabile, si obbliga a comunicare alla cittadinanza l'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, l'eventuale incremento dimensionale dell'impianto e l'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, ai sensi del successivo art. 11, *con un anticipo di **giorni dieci***, mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale.-

3) Gli interessati dovranno essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. *concerti, manifestazioni sportive*). A tal fine si ricorrerà all'utilizzo dello stesso modello semplificato di informativa "**minima**", indicante il titolare del trattamento e la finalità perseguita, già individuato ai sensi dell'art. 13, *comma 3*, del Codice nel provvedimento del 2004 e riportato in *fac-simile* nell'allegato n. 1, al provvedimento dell'8 aprile 2010 e s.m.i. . *Il modello è ovviamente adattabile a varie circostanze. In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, dovranno essere installati più cartelli.*-

Il supporto/cartello con l'informativa:

- dovrà essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;

- dovrà avere un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno; ed un formato e un simbolo identificativo come stabilito dalla direttiva 08.04.2010, del Garante, all. 1 – all. 2, - eventualmente diversificati al fine di informare se le immagini sono registrate, (all. 1) ovvero solo visionate (all. 2).-
- In ogni caso il titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche verbalmente un'informativa adeguata, contenente gli elementi individuati dall'art. 13 del Codice.

Sezione II

DIRITTI DELL'INTERESSATO NEL TRATTAMENTO DEI DATI

Articolo 10

DIRITTI DELL'INTERESSATO/SOGGETTO PRIVATO (vedi anche punto 6. Direttiva Garante)

1) In relazione al trattamento dei dati personali l'*interessato*, dietro presentazione di apposita istanza, ha diritto:

- a) di conoscere l'esistenza di trattamenti di dati che possono riguardarlo;
- b) di essere informato sugli estremi identificativi del titolare e del responsabile oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;
- c) di ottenere, a cura del Responsabile, senza ritardo e comunque non oltre **15 giorni** dalla data di ricezione della richiesta:

I. la conferma dell'esistenza o meno di dati personali che lo riguardano anche se non ancora registrati e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento; la richiesta non può essere inoltrata dallo stesso soggetto se non trascorsi almeno novanta giorni dalla precedente istanza, fatta salva l'esistenza di giustificati motivi;

II. la cancellazione, 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;

III. di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

2) Per ciascuna delle richieste di cui al *comma 1, lett. c), n. 1)*, può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, **un rimborso spese**, equivalente ai costi effettivamente sopportati e comprensivi dei **costi del personale**, definiti con atto formale dalla **Giunta Comunale** secondo le modalità previste dalla normativa vigente.-

3) 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.-

4) Nell'esercizio dei diritti di cui al *comma 1*, l'interessato può conferire, per iscritto specifica delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.-

5) Le istanze di cui al presente articolo possono essere trasmesse al titolare/responsabile anche mediante lettera raccomandata, telefax o posta elettronica, che dovrà provvedere in merito entro e non oltre **15 giorni**.-

6) 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.-

7) Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al Codice, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento (*art. 7 del Codice*). La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal Codice, ovvero nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato (*art. 10, comma 5, del Codice*). 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 (*art. 7, comma 3, lett. a), del Codice*). Viceversa, l'interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge. (*art. 7, comma 3, lett. b), del Codice*).

Articolo 11

SISTEMI INTEGRATI DI VIDEOSORVEGLIANZA (*vedi anche punto 4.6 della Direttiva del Garante*)

Nell'ambito dei predetti trattamenti, sono individuabili le seguenti tipologie di sistemi integrati di videosorveglianza:

a) gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento, i quali utilizzano le medesime infrastrutture tecnologiche; in tale ipotesi, i singoli titolari possono trattare le immagini solo nei casi 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 terzo; tale soggetto terzo, designato responsabile del trattamento ai sensi dell'art. 29 del Codice da parte di ogni singolo titolare, deve assumere un ruolo di coordinamento e gestione dell'attività di videosorveglianza senza consentire, tuttavia, forme di correlazione delle immagini raccolte per conto di ciascun titolare;

c) sia nelle predette ipotesi, sia nei casi in cui l'attività di videosorveglianza venga effettuata da un solo titolare, si può anche attivare un collegamento dei sistemi di videosorveglianza con le sale o le centrali operative degli organi di polizia. ***L'attivazione del predetto collegamento deve essere reso noto agli interessati.*** A tal fine, il Garante ritiene che si possa utilizzare il modello semplificato di informativa "minima" - **indicante il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia**- individuato ai sensi dell'art. 13, *comma 3*, del Codice e riportato in fac-simile nell'*allegato* n. 2 al citato provvedimento del Garante. Tale collegamento deve essere altresì reso noto nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati. Le modalità di trattamento sopra elencate richiedono l'adozione di specifiche misure di sicurezza ulteriori rispetto a quelle individuate nel precedente punto 3.3.1 del citato provvedimento del Garante, quali:

1) 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;

2) Separazione logica delle immagini registrate dai diversi titolari.

Fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno 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/responsabile del trattamento è tenuto a richiedere una verifica preliminare al Garante.

Articolo 12

ULTERIORI AVVERTENZE PER I SISTEMI "INTEGRATI" DI VIDEOSORVEGLIANZA POSTI IN ESSERE DA ENTI PUBBLICI TERRITORIALI DIVERSI.-

Anche gli enti territoriali e, in generale, i soggetti pubblici operanti sul territorio (*es. **Enti Regionali, Provinciali, Religiosi, ecc.***) effettuano attività di videosorveglianza in forma integrata, tramite la compartecipazione ad un medesimo sistema di rilevazione, al fine di economizzare risorse e mezzi impiegati nell'espletamento delle più diverse attività istituzionali.-

Intendendosi, che la Giunta Comunale è autorizzata ad approvare/stipulare apposite convenzioni, con altri Enti pubblici e/o Religiosi, senza fini economici e/o di lucro, qualora vengano riscontrati interessi convergenti riguardanti il posizionamento di un sistema di telecamere di videosorveglianza sul territorio comunale che abbiano una valenza pubblica generale, e non lucrativa/economico-privatistica;

Nel merito il **Garante** ha ben individuato al **punto 4.6** del citato **provvedimento** (*vedi anche punto 5.4 del provvedimento del Garante*) un quadro di specifiche garanzie in ordine alle corrette modalità di utilizzo degli impianti di videosorveglianza e che vengono qui ulteriormente richiamate:

4.6. Sistemi integrati di videosorveglianza

In ottemperanza del principio di economicità delle risorse e dei mezzi impiegati, si è incrementato il ricorso a sistemi integrati di videosorveglianza tra diversi soggetti, pubblici e privati, nonché l'offerta di servizi centralizzati di videosorveglianza remota da parte di fornitori (società di vigilanza, Internet service providers, fornitori di servizi video specialistici, ecc.). Inoltre, le immagini riprese vengono talvolta rese disponibili, con varie tecnologie o modalità, alle forze di polizia.-

Nell'ambito dei predetti trattamenti, sono individuabili le seguenti tipologie di sistemi integrati di videosorveglianza:

a) gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento, i quali utilizzano le medesime infrastrutture tecnologiche; in tale ipotesi, i singoli titolari possono trattare le immagini 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. 29 del Codice da parte di ogni singolo titolare, deve assumere un ruolo di coordinamento e gestione dell'attività di videosorveglianza senza consentire, tuttavia, forme di correlazione delle immagini raccolte per conto di ciascun titolare;

c) sia nelle predette ipotesi, sia nei casi in cui l'attività di videosorveglianza venga effettuata da un solo titolare, si può anche attivare un collegamento dei sistemi di videosorveglianza con le sale o le centrali operative degli organi di polizia. L'attivazione del predetto collegamento deve essere reso noto agli interessati. A tal fine, il Garante ritiene che si possa utilizzare il modello semplificato di informativa "minima" - indicante il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia-individuato ai sensi dell'art. 13, comma 3, del Codice e riportato in fac-simile nell'allegato n. 2 al presente provvedimento. Tale collegamento deve essere altresì reso noto nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati (v. punto 3.1.3).

Le modalità di trattamento sopra elencate richiedono l'adozione di specifiche misure di sicurezza ulteriori rispetto a quelle individuate nel precedente punto 3.3.1, quali:

1) 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.

2) separazione logica delle immagini registrate dai diversi titolari. Il mancato rispetto delle misure previste ai punti 1) e 2) comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-ter, del Codice. Fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno 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 è tenuto a richiedere una verifica preliminare a questa Autorità (v. punto 3.2.1).

Fuori dalle predette ipotesi, il titolare/responsabile del trattamento è tenuto a richiedere una verifica preliminare al Garante, ed in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno 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, agli effetti che possono determinare o, a maggior ragione, con riferimento a quei sistemi per i quali già il punto 3.2.1 del citato provvedimento del Garante la richiede (*es. sistemi di raccolta delle immagini associate a dati biometrici o c.d. intelligenti, cioè in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli*).

Sezione III

SICUREZZA NEL TRATTAMENTO DEI DATI, LIMITI ALL'UTILIZZABILITÀ DEI DATI E RISARCIMENTO DEI DANNI

Articolo 13

SICUREZZA DEI DATI (*vedi anche punto 3.3 della Direttiva del Garante*)

1) I dati personali oggetto di trattamento sono custoditi ai sensi e per gli effetti del precedente art. 6.- Alla sala controllo degli Uffici di Polizia locale dove sono custodite le immagini digitali videoregistrate, può accedere, oltre al Titolare/Responsabile del servizio, il personale di Polizia Locale, debitamente istruito ed incaricato, ai fini delle operazioni del trattamento dei dati ivi registrati.-

2) La sala di controllo è ubicata nell'ufficio del Responsabile della Polizia Locale, e non deve essere direttamente accessibile al pubblico, nella parte adibita alla captazione/registrazione delle immagini.-

3) I dati raccolti mediante sistemi di videosorveglianza dovranno essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini (*artt. 31 e ss. del Codice*).-

Dovranno quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare/responsabile di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (*se soggetto distinto dal titolare/responsabile medesimo, nel caso in cui questo sia persona fisica*).-

Le misure minime di sicurezza dovranno rispettare i seguenti principi:

- a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori **devono essere configurati diversi livelli di visibilità e trattamento delle immagini**. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;
- b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, **deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito**, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
- c) per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;
- d) nel caso di interventi derivanti da esigenze di **manutenzione, occorre adottare specifiche cautele**; in particolare, i soggetti preposti alle predette operazioni potranno accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed **in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini**;

e) qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. **615-ter** del **Codice Penale**;

f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di **tecniche crittografiche** che ne **garantiscono la riservatezza**; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di **connessioni wireless** (*tecnologie wi-fi, wi-max, Gprs*).

A norma delle disposizioni emanate dal Garante **si stabilisce che il titolare/ responsabile deve designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti** e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini.-

Si dovrà trattare di un **numero delimitato** di **soggetti**, specie quando il titolare si avvale di collaboratori esterni, individuando altresì diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (*es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.*). Viene stabilito che, in presenza di differenti competenze specificatamente attribuite ai singoli operatori, devono essere configurati **diversi livelli** di **visibilità** e **trattamento** delle **immagini**. **Laddove tecnicamente possibile**, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, **designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza**.-

Articolo 14

ISTITUTI SCOLASTICI (*vedi anche punto 4.3 della Direttiva del Garante*)

Il sistema di videosorveglianza attivato presso istituti scolastici dovrà garantire il **diritto** dello **studente** alla **riservatezza** (*art. 2, comma 2, D.P.R. n. 249/1998*), prevedendo opportune cautele al fine di assicurare l'armonico sviluppo delle **personalità dei minori** in relazione alla loro vita, al loro processo di maturazione ed al loro **diritto** all'educazione.-

In tale quadro, potrà risultare ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, **al fine di tutelare l'edificio ed i beni scolastici da atti vandalici**, circoscrivendo le riprese alle sole aree interessate **ed attivando gli impianti negli orari di chiusura degli istituti**.-

E' vietato, altresì, attivare le telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgono all'interno della scuola.-

Laddove la ripresa delle immagini riguardi anche le aree perimetrali esterne degli edifici scolastici, l'angolo visuale deve essere delimitato alle sole parti interessate, escludendo dalle riprese le aree non strettamente pertinenti l'edificio.-

Articolo 15

IL DEPOSITO DEI RIFIUTI (*vedi anche punto 5.2 della Direttiva del Garante*)

In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta consentito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose **solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi**.-

Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se 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, l. 24 novembre 1981, n. 689*).

Articolo 16

CESSAZIONE DEL TRATTAMENTO DEI DATI

- 1) In caso di cessazione, per qualsiasi causa, di un trattamento i dati personali sono:
 - a) distrutti;
 - b) ceduti ad altro titolare purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
 - c) conservati per fini esclusivamente istituzionali dell'impianto attivato.
- 2) La cessione dei dati in violazione di quanto previsto dal comma precedente *lett. b)* o di altre disposizioni di legge in materia di trattamento dei dati personali è priva di effetti. Sono fatte salve le sanzioni previste dalla legge.-

Articolo 17

LIMITI ALLA UTILIZZABILITÀ DI DATI PERSONALI (*vedi anche punto 6. Direttiva Garante*)

La materia è disciplinata dall'art. 14 del Codice in materia di protezione dei dati approvato con decreto legislativo 30 giugno 2003 n.196 e s.m.i. e della deliberazione 8 aprile 2010 (10A05072) relativa al **provvedimento** del **Garante** in materia di videosorveglianza pubblicato in Gazzetta Ufficiale nr. 99 del 29/04/2010 e s.m.i. .-

Articolo 18

DANNI CAGIONATI PER EFFETTO DEL TRATTAMENTO DI DATI PERSONALI

La materia è regolamentata per l'intero dall'art. 15 del Codice in materia di protezione dei dati approvato con decreto legislativo 30 giugno 2003 n.196 e s.m.i. e della deliberazione 8 aprile 2010 (10A05072) relativa al **provvedimento** del **Garante** in materia di videosorveglianza pubblicato in Gazzetta Ufficiale nr. 99 del 29/04/2010 e s.m.i. .-

Sezione IV COMUNICAZIONE E DIFFUSIONE DEI DATI

Articolo 19

COMUNICAZIONE

- 1) La comunicazione dei dati personali da parte del Comune di Forgaria nel Friuli 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 delle funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'art. 19 comma 2 del Decreto Legislativo 30/6/2003 n. 196.-
- 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.

CAPO IV TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Articolo 20 TUTELA

1) Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli artt. 100 e seguenti del Decreto Legislativo 30 giugno 2003 n.196 e loro ss.mm.ii..

2) In sede amministrativa, il Responsabile del procedimento, ai sensi e per gli effetti degli artt. 4 e 6 della Legge 7 agosto 1990, n. 241, è il Responsabile del trattamento dei dati personali, così come individuato dal precedente art. 5.-

CAPO V MODIFICHE

Articolo 21 MODIFICHE REGOLAMENTARI

1) I contenuti del presente regolamento dovranno essere aggiornati nei casi di adeguamento normativo in materia di trattamento dei dati personali. Gli eventuali atti normativi, atti amministrativi dell'Autorità di tutela della privacy o atti regolamentari generali del Consiglio Comunale dovranno essere immediatamente recepiti.-

2) All'aggiornamento degli indirizzi vincolati, individuazione aree da sorvegliare, provvederà la Giunta Comunale, ai sensi e per gli effetti di quanto previsto dal vigente ordinamento delle autonomie locali.-

Articolo 22 "Mod. – Schemi - Fac-Simil" operativi:

- 1) DOCUMENTO PER LE SCELTE OPERATE PER L'ATTIVAZIONE DI UN SISTEMA DI VIDEOSORVEGLIANZA DEL TERRITORIO COMUNALE
- 2) SCHEMA NOMINA "RESPONSABILE TRATTAMENTO DEI DATI"
- 3) SCHEMA NOMINA "INCARICATO AL TRATTAMENTO DEI DATI"
- 4) SCHEMA DI LETTERA "ADDETTO ALLA MANUTENZIONE DELL'IMPIANTO DI VIDEOSORVEGLIANZA"
- 5) SCHEMA DI LETTERA "ADDETTO ALLE PULIZIE DEI LOCALI DI VIDEOSORVEGLIANZA"
- 6) SCHEMA "ELENCO TELECAMERE INSTALLATE SUL TERRITORIO"
- 7) SCHEMA DI "RICHIESTA DI ACCESSO ALLE VIDEOREGISTRAZIONI"

- ALLEGATO 1 -

DOCUMENTO PER LE SCELTE OPERATE PER L'ATTIVAZIONE DI UN SISTEMA DI VIDEOSORVEGLIANZA DEL TERRITORIO COMUNALE.

In questo documento sono esplicitate le ragioni che determinano l'implementazione del sistema di videosorveglianza urbana, ovvero la motivazione e le necessità che portano a decidere di installare un impianto di videosorveglianza, specificando anche alcuni aspetti tecnologici, non vincolanti.-
In relazione alle norme dettate dal **Garante** col **provvedimento** generale per la protezione dei dati personali, del **08.04.2010**, *che aggiorna e integra i precedenti del 29.04.2004, e 29.11.2000*, e dal Regolamento Comunale de quo, si determinano le condizioni del sistema di "**video-sorveglianza**" comunale che si va ad adottare, proponendo a base i sotto elencati principi di analisi, gestionali ed operativi; ove il mancato rispetto potrebbe anche determinare la non utilizzabilità del sistema, in particolare l'utilizzabilità dei dati da esso rilevati/registratori/visionati in remoto.-

1. Principio di liceità;

Il sistema deve essere utilizzato esclusivamente per svolgimento, da parte della Polizia Locale, di funzioni istituzionali dell'Ente Comunale (*D.Lgs. 267/2000, Statuto e Regolamenti Comunali vigenti*) nelle fattispecie: prevenzione/repressione attività illecite, sicurezza e tutela del patrimonio, controllo in remoto di fatti anche viabili (*L. 7 marzo 1986 n. 65 "legge quadro sulla Polizia locale" – L.R. 9/2009 e Art. 55 C.P.P.*)-

1.1 Principio di necessità;

Il sistema è progettato e configurato per evitarne usi superflui rispetto agli scopi prefissati. In particolare, i dettagli delle immagini, la durata delle registrazioni, l'identificazione automatica di persone e/o mezzi vanno allineati congruamente agli scopi indicati al punto precedente.- Ciò nel senso che il sistema è predisposto al trattamento di dati anonimi, fintantoché tale non in identificabilità diretta o indiretta consenta di perseguire le finalità di cui al punto precedente.-

1.2 Principio di proporzionalità;

La scelta del sistema di videosorveglianza è preceduta da una valutazione finalizzata a verificare se l'utilizzazione ipotizzata sia in concreto, realmente proporzionata agli scopi prefissi e legittimamente perseguibili.-

Prima di propendere per l'installazione delle telecamere in alcune aree del territorio comunale, si valuterà, con esito negativo, se fossero sufficienti o comunque attuabili altre soluzioni di protezione/prevenzione.-

In particolare il progetto nasce dall'impossibilità di affrontare alcuni fenomeni di micro-criminalità ed altri illeciti, a garanzia e tutela del patrimonio pubblico comunale, (*pleSSI scolastici, impianti sportivi, eco-piazzole, parchi pubblici, aree cimiteriali, punti nevralgici viabili, particolari aree sensibili, ecc.*), ma anche per il controllo, se del caso, del traffico veicolare, con l'ausilio anche di sistemi tradizionali di controllo del territorio.-

La scelta dei punti "sensibili" si determina da esigenze di controllo necessarie a contrastare concreti pericoli per la sicurezza della pubblica incolumità, per scopi di deterrenza o di protezione del patrimonio e allo scopo di identificare in tempo reale/remoto eventuali situazioni di rischio e pericolo per la collettività.-

Il presente sistema di videosorveglianza **non consente** che tramite una integrazione telematica tra più sistemi, si possa ricostruire **percorsi** e/o **abitudini "esclusive"** di un **certo soggetto**; ovvero **irrogare sanzioni amministrative** quali: il calpestio di aiuole, affissioni abusive, ecc. salvo che si tratti di comportamenti tali da compromettere la sicurezza dei cittadini.-

2. Valutazioni, scelte e motivi:

Vanno valutati attentamente i possibili interventi attuabili, considerando in particolare:

- Gli indicatori di eventi criminosi quali: denunce per furti, danneggiamenti, scippi, rapine, atti vandalici, violenze, ecc.-
- L'individuazione delle aree comunali, a destinazione pubblica, a patrimonio pubblico, a maggior rischio.-
- Le indicazioni delle forze di polizia e della cittadinanza relativamente ad aree percepite a rischio sicurezza.-
- Gli orari di maggior rischio.-
- L'intensità del traffico, il numero e la localizzazione dei sinistri stradali e le zone del territorio comunale ove con maggiore frequenza si determinano rischi per la sicurezza civica.-
- Gli strumenti tecnologici e le risorse umane che l'Amministrazione può mettere a disposizione.-
- La razionalizzazione dei compiti che la Polizia Municipale svolge quotidianamente.-
- Le esperienze dirette ed i risultati conseguiti con interventi specifici da parte di altre Amministrazioni Locali nell'ambito della videosorveglianza.-

Trattandosi di attività istituzionale volta in particolare alla prevenzione e documentazione di atti illeciti/vandalici in luoghi pubblici o aperti al pubblico e tutela della sicurezza, necessita di un intervento su un arco di 24/ore continuate.-

Il sistema sarà basato su una centrale operativa con funzioni di controllo e supervisione collocata presso l'ufficio di Polizia locale, dotata di un server per la registrazione delle immagini ed un insieme di punti di ripresa costituiti da telecamere fisse e/o telecontrollabili di tipo "dome" ovvero "brandeggiabili".-

Presso la centrale operativa sarà possibile visualizzare contemporaneamente le immagini di tutte le telecamere, brandeggiare (*in orizzontale ed in verticale*) e zoomare le telecamere soltanto in caso di necessità. Sarà anche possibile visualizzare le registrazioni delle immagini rilevate dalle telecamere stesse soltanto in caso di necessità. -

Il periodo di conservazione delle immagini è stabilito in giorni **7 (sette)**, (*vedi art. 6 Regolamento c./e*) termine che si ritiene essere effettivamente proporzionato al tipo di trattamento svolto, alle finalità dello stesso e al numero effettivo degli addetti alla Polizia Locale rispetto al tempo che potranno in concreto dedicare alle suddette attività di verifica.-

Più precisamente si rappresenta come la scelta di fissare in giorni **7 (sette)** il periodo di durata di conservazione delle immagini dipende dall'impossibilità di garantire la continua presenza di un 'incaricato nella sala di monitoraggio e controllo delle riprese, pur restando la stessa inaccessibile a terzi grazie alla predisposizione di idonee misure di sicurezza.- Ciò, per avere accesso al dato personale e di rilevanza rispetto alle finalità preventivate, anche in remoto.-

Ne consegue che in caso di:

a) dato non rilevante esso verrà distrutto automaticamente dal sistema informatico allo scadere del **settimo** giorno,

b) dato rilevante (*es. atto di vandalismo*) verrà conservato per il tempo necessario (*anche dopo il settimo* giorno) per gli adempimenti successivi (*es. denuncia all'autorità giudiziaria, ecc.*).

L'attività di prevenzione e documentazione di fatti illeciti che interessino la tutela del patrimonio pubblico e del territorio comunale comporterà delle valutazioni geometriche per il posizionamento delle telecamere allo scopo di accertare che il campo ripreso ed i dati personali acquisiti siano congrui con le finalità dell'impianto stesso.- In questo caso si andrà ad individuare delle posizioni ben specifiche atte a raccogliere il massimo di elementi utili a soddisfare le finalità auspiccate, quali un minimo ragionevolmente e tecnicamente possibile di dati personali nel rispetto della privacy e delle direttive del garante.-

I punti di posizionamento della telecamere proposti dal Responsabile di Polizia locale, saranno, di volta in volta, preventivamente, approvati dalla Giunta comunale.-

L'intento del progetto (*disponibilità economica permettendo*) sarà quello di provare ad ottimizzare le risorse umane della polizia locale, grazie alla potenziale possibilità del presidio elettronico continuativo del territorio, alternativo alla presenza fisica del personale di polizia locale, così da permettere anche un monitoraggio remoto sulla viabilità urbana e su aree significative a fini anche di infortunistica stradale.-

3. Aspetti Tecnici:

Le telecamere che si intendono installare, consentono riprese video anche con scarsa illuminazione notturna. Sono finalizzate esclusivamente alla visuale delle zone di pertinenza pubblica.- Per garantire questo principio si valuterà la possibilità di utilizzare telecamere che permettono di oscurare determinati settori di ripresa corrispondenti ad aree private (*es. abitazioni, aziende private, ecc.*).-

Saranno evitate, salvo necessità comprovate di pubblica sicurezza e di polizia giudiziaria, immagini dettagliate, ingrandite o dettagli non rilevanti, nonché la specifica attivazione in modalità automatica delle telecamere per la rilevazione di eventi improvvisi.-

E' opportuna una rivisitazione periodica, preferibilmente con cadenza annuale, per verificare la congruità dei posizionamenti con eventuali modifiche della situazione ambientale.-

Le immagini video riprese dalle telecamere sono trasmesse alla Centrale Operativa tramite una infrastruttura di rete di tipo proprietaria dedicata esclusivamente a questo servizio, wireless o altri sistemi protetti, con trasmissione di tipo digitale, a garanzia dell'impossibilità di intercettare le immagini da parte di malintenzionati o soggetti terzi.-

I segnali video delle unità di ripresa saranno raccolti dalla centrale di monitoraggio e controllo presso l'ufficio di Polizia locale del comune di Forgaria nel Friuli.- In questa sede le immagini saranno visualizzate su monitor e contestualmente registrate su hard disk o altri supporti tecnologici protetti. La videoregistrazione è necessaria per documentare in remoto, eventuali atti criminosi/illeciti/penali, ecc..-

Alla sala di controllo de quo, potrà accedere, solo ed esclusivamente il Responsabile del trattamento dei dati ed il Personale da esso incaricato con delega scritta .-

L'accesso al sistema sarà protetto da **password su più livelli**. - In particolare:

- **Password di amministrazione**, che consente l'assegnazione delle autorizzazioni e delle autenticazioni e la visualizzazione delle immagini registrate, a disposizione unicamente del Responsabile del trattamento;

- **Password di accesso alle funzioni di visualizzazione** ed operatività del sistema, a disposizione del Responsabile e degli Incaricati del trattamento;

Il sistema di videosorveglianza comporterà esclusivamente il trattamento di dati personali rilevati mediante riprese video che, in relazione ai luoghi di installazione delle telecamere, riguarderanno soggetti, mezzi di trasporto ed altre cose, se presenti nell'area interessata dalla sorveglianza.-

- ALLEGATO 2 -

"SCHEMA NOMINA RESPONSABILE DEL TRATTAMENTO DEI DATI"



COMUNE DI FORGARIA NEL FRIULI

Provincia di Udine

Medaglia d'oro al Merito Civile - Eventi sismici 1976

Prot. nr. _____

Gent. Sig.r/a

A MANI

OGGETTO: SISTEMA DI VIDEOSORVEGLIANZA

Nomina di Responsabile del trattamento dei dati personali ai sensi dell'art. 29 del D.Lgs. 30 giugno 2003 n. 196 (Testo Unico sulle disposizioni in materia di protezione dei dati personali).

Il Comune di Forgaria nel Friuli (UD) titolare del trattamento di dati personali nell'ambito del sistema di videosorveglianza sul territorio comunale (in prosieguo semplicemente Titolare),

1. Visto l'art. 29 del D.Lgs. 196/2003, secondo cui il Titolare ha facoltà di designare uno o più responsabili del trattamento dei dati personali, individuandolo/i tra soggetti che per esperienza, capacità e affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

2. Considerato che per la struttura interna del Titolare si ritiene necessaria la nomina di responsabili del trattamento dei dati personali per meglio garantire il rispetto delle norme in materia di Privacy nell'ambito del sistema di videosorveglianza.

3. Considerato che per esigenze organizzative possono essere designati più responsabili, anche mediante suddivisione di compiti.

4. Considerata la sua formazione professionale in materia di privacy si ritiene che Lei sia la persona che meglio risponda ai requisiti di cui al punto 1.

5. Considerato che i compiti affidati al responsabile sono per legge analiticamente specificati per iscritto dal titolare

Tutto ciò premesso e considerato,

la presente vale a conferirLe ad ogni effetto di legge formale ed espressa nomina a responsabile del trattamento dei dati personali trattati nell'ambito ed in stretta pertinenza alle prestazioni dedotte nel contratto di lavoro stipulato con la scrivente Amministrazione e con specifico riguardo del sistema di videosorveglianza, così come disciplinato dal relativo Regolamento, approvato con Deliberazione Consiliare n. ____ del _____ e nell'ambito delle finalità ivi dettagliate e qui integralmente richiamate.

Lei, in qualità di responsabile è tenuto ad effettuare il trattamento nei limiti delle finalità individuate nel predetto Regolamento Comunale attenendosi alle istruzioni impartite dal Titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle proprie istruzioni.

Perché sia garantito un adeguato trattamento dei dati personali di cui è titolare la scrivente Amministrazione, è opportuno che Lei, a cui viene affidato il trattamento nell'espletamento dell'incarico conferito ne assuma la responsabilità anche ai fini e sotto il profilo della sicurezza prescritta dalla summenzionata normativa, con

particolare riferimento all'adozione delle misure di sicurezza minime e idonee atte a garantire la sicurezza, integrità e riservatezza dei dati personali ed all'assegnazione di specifiche istruzioni agli incaricati atte a garantire il rispetto delle misure medesime.

Nello svolgimento dell'incarico dovrà attenersi alle istruzioni impartite dal titolare e a sua volta impartire agli incaricati le opportune istruzioni per rispettare tutti gli obblighi di legge, compreso il profilo della sicurezza, quali:

1. individuare e autorizzare per iscritto gli incaricati e l'ambito di trattamento dei dati loro consentito sulla base delle rispettive mansioni ed assegnare ai medesimi istruzioni scritte atte ad assicurare un corretto trattamento al fine di preservare la riservatezza dei dati;
2. adempiere agli obblighi di informativa e, ove richiesto, di acquisizione del consenso nei confronti degli interessati;
3. garantire agli interessati l'esercizio dei diritti previsti dall'art. 7 del d.lgs. n.196/2003, fra cui quelli di accesso, aggiornamento, rettificazione, cancellazione e di opposizione;
4. collaborare con il titolare all'attuazione di eventuali prescrizioni del Garante; predisporre ed aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni di cui agli artt. 31 e ss del d.lgs. n. 196/2003 e del Disciplinare Tecnico di cui all'Allegato B, curandone l'applicazione anche da parte degli incaricati;
5. comunicare, ove richiesto, al Titolare le modalità e finalità di gestione del trattamento dei dati, fermo restando che la comunicazione e diffusione dei dati personali può essere effettuata previa autorizzazione del titolare;
6. predisporre la notificazione al Garante, ove obbligatoria;
7. verificare l'esattezza e la completezza dei dati, apportando tempestivamente eventuali variazioni ed aggiornamenti;
8. osservare le disposizioni contenute nelle autorizzazioni generali del Garante nel trattamento di dati sensibili e/o giudiziari.

Il responsabile così nominato dichiara di essere consapevole che i dati che tratta nell'espletamento dell'incarico ricevuto sono dati personali e, come tali, sono soggetti all'applicazione del codice per la protezione dei medesimi di cui al D. Lgs. 196/2003, e, per l'effetto, di ottemperare a tutti gli obblighi previsti dalla predetta normativa.

Il Titolare

Il responsabile

**- ALLEGATO 3 -
SCHEMA NOMINA "INCARICATO AL TRATTAMENTO DEI DATI"**



COMUNE DI FORGARIA NEL FRIULI

Provincia di Udine

Medaglia d'oro al Merito Civile - Eventi sismici 1976

Prot. nr. _____

Gent. Sig.r/a

A MANI

OGGETTO: SISTEMA DI VIDEOSORVEGLIANZA
Nomina di incaricato al trattamento dei dati personali ai sensi dell'art. 30 del D.Lgs. 30 giugno 2003 n. 196 (Testo Unico sulle disposizioni in materia di protezione dei dati personali).

Ai sensi dell'art. 30 del D.Lgs. 196/2003 il trattamento dei dati personali nell'ambito del sistema di videosorveglianza sul territorio comunale può essere effettuato solo da soggetti espressamente incaricati, che operano sotto la diretta autorità del titolare o del responsabile eventualmente nominato, e che si attengono alle istruzioni dai medesimi impartite. Per incaricati devono intendersi le persone fisiche autorizzate a compiere operazioni di trattamento dei dati dal titolare o dal responsabile nei limiti delle finalità indicate nel Regolamento Comunale sulla Videosorveglianza, approvato con Deliberazione Consiliare n. ___ del _____.

La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito, per tale intendendosi anche la preposizione dell'incaricato ad un'unità operativa per la quale è individuato l'ambito del trattamento consentito agli addetti all'unità medesima.

Ciò premesso, la presente vale a conferire ad ogni effetto di legge formale ed espressa nomina ad incaricato del trattamento dei dati personali gestiti nell'ambito ed in stretta pertinenza alle prestazioni dedotte nel contratto di lavoro stipulato con la scrivente Amministrazione e con specifico riguardo al sistema di videosorveglianza così come disciplinato dal relativo Regolamento, approvato con Deliberazione Consiliare n. ___ del _____ e nell'ambito delle finalità ivi dettagliate e qui integralmente richiamate.

Per effetto ed ai fini del conferimento del presente incarico, è compito del titolare, eventualmente con l'ausilio e in collaborazione con uno o più responsabili, fornire alla persona così designata una serie di informazioni ed istruzioni volte all'assolvimento degli obblighi previsti dalla normativa di cui al D.Lgs. 196/2003, atte a garantire un trattamento lecito e protetto dei dati personali e in particolare l'adozione di una serie di misure di sicurezza nello svolgimento delle rispettive mansioni lavorative e del corrispondente ambito di trattamento dei dati, onde evitare rischi di distruzione, perdita, accessi non autorizzati e trattamenti non consentiti dei dati medesimi.

In particolare, vengono date le seguenti informazioni:

Definizione di trattamento con strumenti elettronici: trattamento dei dati comprende qualunque operazione o complesso di operazioni eseguita con strumenti elettronici, che implichi il coinvolgimento dei dati personali, ivi compresa la raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e distruzione dei dati personali, anche ove non registrati in banche dati.

Definizione di dato personale: per dato personale si intende qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Definizione di dato sensibile: per dato sensibile si intende in particolare il dato idoneo a rivelare origine razziale ed etnica, convinzioni religiose e ideologiche, opinioni politiche, adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, stato di salute e vita sessuale. Interessato è la persona fisica, persona giuridica, ente o associazione, cui si riferiscono i dati personali.

Vengono inoltre impartite le seguenti istruzioni:

- l'incaricato deve trattare i dati personali contenuti in supporti informatici, avendo cura che l'accesso ai medesimi sia possibile solo ai soggetti autorizzati;
- in caso di interruzione anche solo temporanea di propria attività lavorativa che comporti il trattamento di dati personali, l'incaricato non deve lasciare incustodito il supporto elettronico contenente i dati medesimi, sì da evitare accessi e utilizzi illeciti;
- deve concorrere ad adempiere agli obblighi di informativa nei confronti degli interessati, e a garantire agli interessati l'esercizio dei diritti previsti dall'art. 7 del d.lgs. n.196/2003, fra cui quelli di accesso, aggiornamento, rettificazione, cancellazione e di opposizione;
- deve verificare l'esattezza e la completezza dei dati;
- deve collaborare con il titolare all'attuazione di eventuali prescrizioni del Garante;
- concorrere all'applicazione di un sistema di sicurezza idoneo a rispettare le prescrizioni di cui agli artt. 31 e ss del d.lgs. n. 196/2003 e del Discipline Tecnico di cui all'Allegato B.

Le misure minime di protezione da osservare con riferimento al trattamento di dati effettuato con strumenti elettronici, consistono nel rispetto delle procedure predisposte dall'Amministrazione per la tutela del sistema informatico, ovvero delle procedure di autenticazione informatica, di gestione delle credenziali di autenticazione, di utilizzazione di un sistema di autorizzazione per l'accesso alle banche dati, di aggiornamento periodico dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione e manutenzione degli strumenti elettronici, di protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti e accessi non consentiti, di custodia di copie di sicurezza e di ripristino della disponibilità dei dati e dei sistemi, di tenuta di un aggiornato documento programmatico sulla sicurezza. Ad ogni incaricato è assegnata in via riservata una credenziale per l'autenticazione (password) che consente l'accesso ai dati, e che non va comunicata ad altri incaricati; l'incaricato deve assicurare la segretezza della credenziale di autenticazione e la diligente custodia dei dispositivi in possesso ed uso esclusivo; la parola chiave prevista dal sistema di autenticazione, composta da almeno otto caratteri o da un numero di caratteri pari al massimo consentito dallo strumento elettronico in dotazione, non contiene riferimenti agevolmente riconducibili all'incaricato; è modificata al primo utilizzo e successivamente almeno ogni sei mesi e ogni tre mesi se si trattano anche dati sensibili; le variazioni disposte autonomamente dallo stesso incaricato con periodicità semestrale (trimestrale in caso di trattamento di dati sensibili o giudiziari) devono essere comunicate, sempre in modo riservato, al custode delle credenziali. Il codice di identificazione una volta utilizzato non può essere assegnato ad altri incaricati neppure in tempi diversi. Le credenziali non utilizzate da almeno sei mesi sono disattivate salvo quelle preventivamente autorizzate dal titolare per i soli scopi di gestione tecnica; le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali. Lo strumento elettronico in dotazione non va lasciato incustodito e accessibile durante il trattamento dei dati; tutti i supporti magnetici utilizzati vanno riposti negli archivi; i supporti non più utilizzati possono essere eliminati solo dopo che i dati contenuti sono stati resi effettivamente inutilizzabili. L'incaricato non può installare ed utilizzare programmi per elaboratore non autorizzati dall'Amministrazione. Gli strumenti informatici e telematici messi a disposizione costituiscono degli strumenti di lavoro da utilizzare esclusivamente per l'esecuzione delle mansioni affidate. Il titolare del trattamento, nei casi in cui è indispensabile ed indifferibile accedere ai dati trattati dall'incaricato ed agli strumenti informatici in dotazione allo stesso per la sicurezza ed operatività dello stesso sistema informatico, nei casi di prolungata assenza od impedimento dell'incaricato, potrà accedere mediante intervento del custode delle credenziali nominato dall'azienda.

I dati personali devono essere custoditi con la massima riservatezza, diligenza e prudenza e in nessun modo divulgati al di fuori delle espresse autorizzazioni del titolare o del responsabile.

Gli accessi alle banche dati sia informatiche che cartacee e agli archivi, così come la comunicazione dei dati personali che l'incaricato è autorizzato ad effettuare, sono solo quelle strettamente pertinenti e finalizzate alle specifiche mansioni svolte; l'accesso ai dati deve essere limitato all'espletamento delle proprie mansioni ed inoltre esclusivamente negli orari di lavoro. I dati personali devono essere infatti trattati unicamente per le finalità inerenti le proprie prestazioni lavorative.

Analogamente, senza preventiva autorizzazione del titolare non è permesso all'incaricato realizzare nuove banche dati, o trattare le medesime per finalità diverse da quelle pertinenti alle sue mansioni. Gli obblighi di riservatezza dei dati devono essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro..

Il titolare Comune di Forgaria nel Friuli

L'incaricato

- ALLEGATO 4 -

SCHEMA "ADDETTO ALLA MANUTENZIONE DELL'IMPIANTO DI VIDEOSORVEGLIANZA"



COMUNE DI FORGARIA NEL FRIULI

Provincia di Udine

Medaglia d'oro al Merito Civile - Eventi sismici 1976

Prot. nr. _____

Gent. Sig.r/a
Nome e Cognome

A MANI

OGGETTO: ADDETTO ALLA "MANUTENZIONE" DEL SISTEMA DI VIDEOSORVEGLIANZA
artt. 33 e ss. del D.lgs. 30 giugno 2003 n. 196 e al Discipline tecnico di cui all' Allegato B
(Testo Unico sulle disposizioni in materia di protezione dei dati personali)

La scrivente Amministrazione si avvale con specifico riguardo del sistema di videosorveglianza - così come disciplinato dal relativo Regolamento, approvato con Deliberazione Consiliare n. ___ del _____ e nell'ambito delle finalità ivi dettagliate e qui integralmente richiamate - di prestatori di servizi che, pur non effettuando ai sensi di legge trattamento di dati personali di cui è titolare la stessa committente, devono opportunamente essere responsabilizzati e informati, sia pur sinteticamente, dei rischi che incombono sulla sicurezza dei dati e delle misure di sicurezza prescritte dalla legge e predisposte dal titolare al fine di conformarsi alla normativa sulla protezione dei dati personali.

Con la presente si intende preservare la liceità e correttezza del trattamento dei dati personali, sia su supporto cartaceo che elettronico anche rispetto all'espletamento delle mansioni dei prestatori di servizi esterni alla struttura del titolare.

Il prestatore di servizi dichiara di essere consapevole di espletare le mansioni all'interno di una struttura in cui viene effettuato il trattamento di dati personali, rilevante ai fini del Testo Unico in materia di riservatezza sopra citato, e per l'effetto, di essere tenuto sia pur in stretta pertinenza alle mansioni stesse, a rispettare le misure di sicurezza prescritte dalla legge per preservare la riservatezza dei dati medesimi, tra cui la diligente gestione, custodia e conservazione di documenti cartacei e informatici così come dei locali contenenti dati personali, di limitarsi strettamente e unicamente allo svolgimento delle mansioni conferite nella consapevolezza che nulla hanno a che condividere con il trattamento di dati personali, e dei limiti che ne derivano, tra cui in particolare, è fatto divieto assoluto di far fuoriuscire ogni genere di documento di qualsiasi foggia e natura dai locali in cui gli stessi vengono per qualsiasi ragione e in qualunque modo occasionalmente o volutamente rinvenuti; di accedere o anche solo tentare di accedere a supporti cartacei ed elettronici di qualsiasi tipo e genere rinvenuti nei locali medesimi; di comunicare o diffondere il contenuto di documenti rinvenuti nei locali contravvenendo alle misure di sicurezza predisposte dal titolare; si richiede altresì di non lasciare incustoditi i locali neppure temporaneamente sì da impedire accessi non autorizzati; avere cura di chiudere ogni via di accesso ai locali durante e al termine delle proprie mansioni; di non toccare, intaccare, danneggiare, asportare, dislocare, supporti cartacei e elettronici di qualsiasi dimensione, foggia e natura; di non avvalersi per l'espletamento delle proprie mansioni, di soggetti non previamente autorizzati nel rapporto contrattuale con il titolare e vigilare in ogni caso costantemente sull'attività dei medesimi all'interno dei locali.

Il tutto a pena di responsabilità civili e penali in caso di inosservanza delle prescrizioni succitate e di ogni altra conseguente, connessa e correlata ai fini del testo unico in materia di protezione dei dati personali, ferma restando la risoluzione ipso iure del rapporto contrattuale in essere con il titolare.

Il Titolare _____

Il prestatore di servizi _____

**- ALLEGATO 5 -
SCHEMA "ADDETTO ALLE PULIZIE DEI LOCALI DI VIDEOSORVEGLIANZA"**



COMUNE DI FORGARIA NEL FRIULI

Provincia di Udine

Medaglia d'oro al Merito Civile - Eventi sismici 1976

Prot. nr. _____

Gent. Sig.r/a
Nome e Cognome

A MANI

OGGETTO: ADDETTO ALLE PULIZIE DEI LOCALI DI VIDEOSORVEGLIANZA

artt. 33 e ss. del D.lgs. 30 giugno 2003 n. 196 e al Discipline tecnico di cui all' Allegato B
(*Testo Unico sulle disposizioni in materia di protezione dei dati personali*)

La scrivente Amministrazione si avvale di prestatori di servizi che, pur non effettuando ai sensi di legge trattamento di dati personali di cui è titolare la stessa committente, devono opportunamente essere responsabilizzati e informati, sia pur sinteticamente, dei rischi che incombono sulla sicurezza dei dati e delle misure di sicurezza prescritte dalla legge e predisposte dal titolare al fine di conformarsi alla normativa sulla protezione dei dati personali.

Con la presente si intende preservare la liceità e correttezza del trattamento dei dati personali, sia su supporto cartaceo che elettronico anche rispetto all'espletamento delle mansioni dei prestatori di servizi esterni alla struttura del titolare.

Il prestatore di servizi dichiara di essere consapevole di espletare le mansioni all'interno di una struttura in cui viene effettuato il trattamento di dati personali, rilevante ai fini del Testo Unico in materia di riservatezza sopra citato, e per l'effetto, di essere tenuto sia pur in stretta pertinenza alle mansioni stesse, a rispettare le misure di sicurezza prescritte dalla legge per preservare la riservatezza dei dati medesimi, tra cui la diligente gestione, custodia e conservazione di documenti cartacei e informatici così come dei locali contenenti dati personali, di limitarsi strettamente e unicamente allo svolgimento delle mansioni conferite nella consapevolezza che nulla hanno a che condividere con il trattamento di dati personali, e dei limiti che ne derivano, tra cui in particolare, è fatto divieto assoluto di far fuoriuscire ogni genere di documento di qualsiasi foggia e natura dai locali in cui gli stessi vengono per qualsiasi ragione e in qualunque modo occasionalmente o volutamente rinvenuti; di accedere o anche solo tentare di accedere a supporti cartacei ed elettronici di qualsiasi tipo e genere rinvenuti nei locali medesimi; di comunicare o diffondere il contenuto di documenti rinvenuti nei locali contravvenendo alle misure di sicurezza predisposte dal titolare; si richiede altresì di non lasciare incustoditi i locali neppure temporaneamente sì da impedire accessi non autorizzati; avere cura di chiudere ogni via di accesso ai locali durante e al termine delle proprie mansioni; di non toccare, intaccare, danneggiare, asportare, dislocare, supporti cartacei e elettronici di qualsiasi dimensione, foggia e natura; di non avvalersi per l'espletamento delle proprie mansioni, di soggetti non previamente autorizzati nel rapporto contrattuale con il titolare e vigilare in ogni caso costantemente sull'attività dei medesimi all'interno dei locali.

Il tutto a pena di responsabilità civili e penali in caso di inosservanza delle prescrizioni succitate e di ogni altra conseguente, connessa e correlata ai fini del testo unico in materia di protezione dei dati personali, ferma restando la risoluzione ipso iure del rapporto contrattuale in essere con il titolare.

Il Titolare _____

Il prestatore di servizi _____

**- ALLEGATO 6 -
SCHEMA "ELENCO TELECAMERE INSTALLATE SUL TERRITORIO COMUNALE"**

Il sistema si compone di una rete di comunicazioni dati, via etere, via cavo, anche tramite tecnologia "wireless" e di telecamere connesse alla sala di controllo posta presso l'ufficio di Polizia locale del comune di Forgaria nel Friuli. Il sistema è a circuito chiuso e i relativi elaboratori non sono interconnessi con altri sistemi, archivi o banche dati, né sono accessibili da altre periferiche.-

Fatto salvo la possibilità di collegamento del "sistema" con la sede operativa di Protezione Civile di Palmanova, ovvero con altre forze di Polizia dello stato, quali potrebbero essere il Comando Carabinieri di San Daniele del Friuli e il Commissariato di Polizia di Tolmezzo o Udine.-

POSTAZIONE	Tipo	Modello	Descrizione
Nr. 1 : Municipio – Piazza Tre Martiri	Brandeggiabile		Telecamera con teleobiettivo
Nr. 2 : Area scolastica – centro sportivo	Brandeggiabile		Telecamera con teleobiettivo
Nr. 3 : Ecopiazzola	Brandeggiabile		Telecamera con teleobiettivo

**- ALLEGATO 7 -
SCHEMA "RICHIESTA DI ACCESSO ALLE VIDEOREGISTRAZIONI"**



COMUNE DI FORGARIA NEL FRIULI

Provincia di Udine

Medaglia d'oro al Merito Civile - Eventi sismici 1976

AI RESPONSABILE DEL SERVIZIO
DI POLIZIA LOCALE

Il sottoscritto
nato a, il
residente in via Nr.
Identificato tramite Nr. Rilasciata il Da,
ai sensi della vigente normativa di privacy, richiede di esercitare il diritto di accesso alle immagini video che
potrebbero aver registrato dati personali a sé stesso afferenti.

Per permettere di individuare tali immagini nell'archivio video, fornisce le seguenti informazioni:

1. Luogo o luoghi di possibile ripresa:
 2. Data di possibile ripresa:
 3. Fascia oraria di possibile ripresa (*approssimazione di 30 minuti*):
 4. Abbigliamento al momento della possibile ripresa:
 5. Accessori (*borse, ombrelli, carrozzine, animali al guinzaglio, altri oggetti*):
 6. Presenza di accompagnatori (*indicare numero, sesso, sommaria descrizione*):
 7. Attività svolta durante la ripresa:
- Recapito (o *contatto telefonico*) per eventuali approfondimenti:

In fede.
(firma) _____

Forgaria nel Friuli, li,

Allegare: copia carta d'Identità del richiedente, in corso di validità.-

PARTE DA CONSEGNARE AL RICHIEDENTE

In data alle ore - ns. Prot. dd.
il/la Sig./Sig.ra
ha avanzato richiesta di accesso a videoregistrazioni, ai sensi della vigente normativa in materia di privacy.

(*firma del ricevente la richiesta*)