Comune di
Omignano

Allegato alla delibera C.C. numero 22 del 20.08.2020

Regolamento Comunale Videosorveglianza

In ossequio alla normativa vigente, si informa e si prende atto che l'Ente con diffusione anche con comunicazione a distanza ha già provveduto a rendere la seguente informativa ex artt. 13 e 14 GDPR UE 679/2016:

INFORMATIVA (allegato 1)

In questa pagina si descrivono le modalità di gestione del sito in riferimento al trattamento dei dati personali degli utenti che lo consultano. Si tratta di un'informativa per la protezione dei dati personali resa anche ai sensi dell'art. 14 del Regolamento UE 2016/679 (d'ora in poi GDPR) e del DLGS 101/2018 a coloro che interagiscono con i servizi web del sito istituzionale del Comune di Omignano per la protezione dei dati personali, accessibili per via telematica a partire dall'indirizzo: www.comuneomignano.it

L'informativa è resa solo per il sito indicato e non anche per altri siti web eventualmente consultabili dall'utente tramite link.

L'informativa è resa completa in virtu' anche della Raccomandazione n. 2/2001 che le Autorità Europee per la Protezione dei Dati Personali, riunite nel "Gruppo" istituito dall'art. 29 della direttiva n. 95/46/CE, hanno adottato il 17 maggio 2001 per individuare alcuni requisiti minimi per la raccolta di dati personali on-line e, in particolare, le modalità, i tempi e la natura delle informazioni che i titolari del trattamento devono fornire agli utenti quando questi si collegano a pagine web, indipendentemente dagli scopi del collegamento.
Lo scopo della presente informativa privacy è fornire in maniera trasparente notizie sui dati raccolti eventualmente dal sito e sulle relative modalità di utilizzo.
La consultazione di questo sito da parte dell'utente, puo' comportare il rilascio di informazioni aventi natura di dati personali.

Per tali finalità il Titolare del trattamento è:

- il Comune di Omignano , con sede in Via Europa, 16 Omignano (SA) CF 81001810654 nella persona del Sindaco pro-tempore Dott. Raffaele Mondelli sindaco©comuneomignano.gov.it

-Il Responsabile Protezione Dati : RPD Micael Polito domiciliato per la carica presso l'ente (politoconsulting©yahoo.com; micaelpolito©pec.it)

I dati personali dell'utente sono trattati da soggetti autorizzati dal Titolare del trattamento e da incaricati e responsabili appositamente nominati e istruiti dall'Ente in qualità di Titolare, autorizzati ad accedervi in forza di disposizioni di legge, regolamenti e normative.
I dati personali dell'utente sono altresì trattati dai soggetti designati eventualmente in qualità di Amministratori di sistema (incaricati) ai sensi del Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 e ss.mm.ii.

FINALITÀ E MODALITÀ DI TRATTAMENTO

I dati personali verranno trattati per mezzo di strumenti informatico/telematici per finalità strettamente necessarie alla consultazione del sito www.comuneomignano.it nonché per finalità connesse e/o strumentali alla consultazione stessa. Tali dati sono trattati in forma automatizzata e raccolti in forma esclusivamente aggregata al fine di verificare il corretto funzionamento del sito, nonché per motivi di sicurezza.

Il trattamento dei dati avverrà per mezzo di strumenti e con modalità volte ad assicurare la riservatezza e la sicurezza dei dati, nel rispetto di quanto definito negli articoli 32 e ss. del GDPR ed in conformità con la normativa nazionale vigente in materia.

Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

BASE GIURIDICA E LICEITÀ DEL TRATTAMENTO

Il trattamento dei dati personali per le finalità di cui sopra non richiede il consenso in quanto necessario per consentire la consultazione del sito www.comuneomignano.it
I dati personali forniti dagli utenti che inoltrano richieste di eventuale registrazione al sito sono utilizzati al solo fine di eseguire il servizio o la prestazione richiesta. I dati eventualmente forniti dall'utente in particolari sezioni del presente sito non vengono memorizzati in maniera persistente sui server.

LUOGO DI TRATTAMENTO DEI DATI

I trattamenti connessi ai servizi web di questo sito hanno luogo presso la predetta sede del Titolare al trattamento e presso le sedi fisicamente designate dagli host (con reindirizzamento automatico eventuale) individuati in luogo del titolare e curati solo da personale tecnico della struttura responsabile del trattamento, oppure da eventuali soggetti autorizzati ad effettuare occasionali operazioni di manutenzione. Nessun dato derivante dal servizio web viene comunicato o diffuso a terzi.

TIPOLOGIA DI DATI TRATTATI E RELATIVI TEMPI DI CONSERVAZIONE

Dati di navigazione

I sistemi informatici e le procedure software preposte al funzionamento di questo sito web possono acquisire, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet. Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti. In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (*Uniform Resource Identifier*) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine,

errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.

Dati forniti volontariamente dall'utente

L'invio facoltativo, esplicito e volontario di posta elettronica agli indirizzi indicati su questo sito comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella missiva.
Tali dati sono conservati per il tempo necessario ad evadere le richieste pervenute. Trascorsi tali termini i Suoi dati saranno anonimizzati o cancellati, salvo che non ne sia necessaria la conservazione per altre e diverse finalità previste per espressa previsione di legge (ad es. finalità di archiviazione).

Cookies

Nessun dato personale degli utenti viene in proposito acquisito dal sito.
Non viene fatto uso di cookies per la trasmissione di informazioni di carattere personale, né vengono utilizzati c.d. cookies persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.
L'uso di c.d. cookies di sessione (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del browser) è strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal server) necessari per consentire l'esplorazione sicura ed efficiente del sito.
I c.d. cookies di sessione utilizzati in questo sito evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificativi dell'utente.
Per avere maggiori informazioni sulla tipologia di cookie utilizzati, le finalità e le modalità di disabilitazione è possibile consultare la sezione specifica.

NATURA DEL CONFERIMENTO E CONSEGUENZE DEL RIFIUTO

A parte quanto specificato per i dati di navigazione, l'utente è libero di fornire al Comune di Omignano i dati personali riportati eventualmente in moduli di richiesta o comunque indicati in contatti con l'Ente per sollecitare l'invio di materiale informativo o di altre comunicazioni.
Pertanto, l'eventuale rifiuto del conferimento dei dati obbligatori comporterà l'oggettiva impossibilità di perseguire le finalità di trattamento di cui alla presente Informativa e di ottenere quanto richiesto.
Per completezza va ricordato che in alcuni casi (non oggetto dell'ordinaria gestione di questo sito) l'Autority può richiedere notizie e informazioni ai fini del controllo sul trattamento dei dati personali. In questi casi la risposta è obbligatoria a pena di sanzione amministrativa.

DIRITTI DELL' INTERESSATO

Ai sensi e per gli effetti di cui al GDPR, Le sono riconosciuti i seguenti diritti in qualità di Interessato che potrà esercitare nei confronti dell'Ente:

a. diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che La riguardano e, in tal caso, di ottenere l'accesso ai dati personali e alle informazioni previste dall'art. 15 del GDPR ed in particolare a quelle relative alle finalità del trattamento, alle categorie di dati personali in questione, ai destinatari o categorie di destinatari a cui i dati personali sono stati o saranno comunicati, al periodo di conservazione, etc.;
b. diritto di ottenere, laddove inesatti, la rettifica dei dati personali che La riguardano, nonché l'integrazione degli stessi laddove ritenuti incompleti sempre in relazione alle finalità del trattamento (art. 16);
c. diritto di cancellazione dei dati ("diritto all'oblio"), laddove ricorra una delle fattispecie di cui all'art. 17;
d. diritto di limitazione del trattamento, nei casi previsti dall'art. 18;
e. diritto di portabilità dei dati ai sensi dell'art. 20;
f. diritto di opposizione al trattamento ai sensi dell'art. 21;
g. diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, solamente per le finalità la cui base giuridica è il consenso (art. 7).

Tali diritti potranno essere esercitati mediante richiesta inviata con lettera raccomandata a.r. al Responsabile della Protezione dei Dati (RPD) al seguente indirizzo: DPO presso Comune Omignano , o mediante e-mail al seguente indirizzo di posta elettronica: micaelpolito©pec.it, utilizzando l'apposito modulo disponibile sul sito dell'Autorità Garante per la protezione dei dati personali www.garanteprivacy.it/home/modulistica-e-servizi-online

Si ricorda, infine, che Lei ha il diritto di proporre reclamo al Garante per la Protezione dei dati personali o ad altra Autorità di controllo ai sensi dell'art. 13, par. 2, lettera d) del GDPR

MODIFICHE ALLA PRESENTE INFORMATIVA

La presente Informativa può subire variazioni. Si consiglia, quindi, di controllare regolarmente la sezione privacy per la verifica dell'aggiornamento

****

PRINCIPI GENERALI REGOLAMENTO VIDEOSORVEGLIANZA COMUNE DI OMIGNANO

Art. 1 – Premessa

In riscontro alla presenza di telecamere sul territorio appartenenti al sistema di videosorveglianza già adottato dall'Ente, si specifica che le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto a cui si riferiscono, costituiscono dati personali. La videosorveglianza dà luogo pertanto a trattamento di dati personali e incide sul diritto alla riservatezza delle persone fisiche eventualmente presenti nell'area sottoposta a ripresa.

Il presente Regolamento garantisce che il trattamento dei dati personali, effettuato mediante sistemi di videosorveglianza gestiti ed impiegati dal Comune di Omignano nel territorio comunale, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

Art. 2 - Norme di riferimento e principi generali

Il presente regolamento disciplina il trattamento di dati personali, realizzato mediante l'impianto di videosorveglianza cittadina, attivato nel territorio del Comune di Omignano (SA)

Per tutto quanto non dettagliatamente disciplinato dal presente Regolamento, si rinvia a quanto disposto dal:

- Regolamento UE Generale sulla Protezione dei Dati 2016/679 (di seguito RGPD) relativo "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";
- Direttiva UE 2016/680 relativa "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati";
- Dlgs. 101/2018, recante l'individuazione delle modalità di attuazione dei principi del GDPR UE 679/2016 in materia di protezione dei dati personali relativamente anche alla compatibilità del trattamento dei dati effettuato per le finalità di polizia da organi, uffici e comandi di polizia municipale ;
- Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell'8 aprile 2010 (G.U. n. 99 del 29/04/2010);

- Decreto Ministero dell'Interno 05/08/2008 (GU n. 186 del 09.08.2008);
- Legge n. 38/2009 recante "misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale nonché in tema di atti persecutori".

La Videosorveglianza in ambito Comunale si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5, RGDP e, in particolare:

-Principio di liceità – Il trattamento di dati personali da parte di soggetti pubblici è lecito allorquando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento in ossequio al disposto di cui all'art. 6, Paragrafo 1, lett. e), RGPD.
La videosorveglianza comunale pertanto è consentita senza necessità di consenso da parte degli interessati.

-Principio di necessità – In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati(c.d. minimizzazione dei dati) di cui all'art. 5, Paragrafo 1, lett. c), RGPD, il sistema di videosorveglianza, i sistemi informativi ed i programmi informatici utilizzati, sono configurati per ridurre al minimo l'utilizzazione di dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di videosorveglianza. Inoltre, qualora non sia necessario individuare le persone, i sistemi devono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, con riprese di insieme e, il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati.

-Principio di proporzionalità – La raccolta e l'uso delle immagini devono essere proporzionali agli scopi perseguiti. In applicazione dei principi di proporzionalità e di necessità, nel procedere alla commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un'effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento.

Nell'uso delle apparecchiature volte a riprendere, per i legittimi interessi indicati, aree esterne ed edifici, il trattamento deve essere effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da proteggere.

-Principio di finalità – Ai sensi dell'art. 5, Paragrafo 1, lett. b), RGPD,i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. E' consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la sicurezza urbana che il DM Interno 05/08/2008 definisce come il "*bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale.*" *(anche richiamato in altra specifica)

Art. 3 – Definizioni

Ai fini del presente Regolamento si intende:

- per «**dato personale**», qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

- per «**trattamento**», qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- per "**banca dati**", il complesso organizzato di dati personali, formatosi attraverso le apparecchiature di registrazione e ripresa video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nelle aree interessate dalle riprese;

- per «**profilazione**», qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute,

le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

- per «**pseudonimizzazione**», il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

- per «**titolare del trattamento**», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- per «**responsabile del trattamento**», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- per «**incaricato del trattamento**», la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del titolare o del responsabile del trattamento;

- per "**interessato**", la persona fisica cui si riferiscono i dati personali oggetto di trattamento;

- per «**terzo**», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

- per «**violazione dei dati personali**», la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accessoai dati personali trasmessi, conservati o comunque trattati;

- per "**comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

- per "**diffusione**", il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

- per "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
- il «**Titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
  - il «**Responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
  - l'**autorizzato del trattamento** - la persona fisica autorizzata a compiere operazione di trattamento dal Titolare o dal Responsabile . Il regolamento GDPR , però, prevede per il Titolare **l'obbligo di formare gli addetti autorizzati al trattamento** dei dati ed inoltre, in termini di misure tecniche e organizzative di sicurezza.
- il **Data ProtectionOfficer** figura atta a garantire la conformità di circolazione e protezione dei dati rispetto alle vigenti leggi in materia.

Art. 4 – Finalità istituzionali dei sistemi di videosorveglianza

Le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza attengono allo svolgimento delle funzioni istituzionali proprie dell'amministrazione comunale in conformità a quanto previsto dal:

- D. Lgs. 18 agosto 2000, n. 267 – TUEL
- D.P.R. 24 luglio 1977, n. 616;
- D. Lgs. 31 marzo 1998, n. 112;
- Legge 7 marzo 1986, n. 65, sull'ordinamento della Polizia Municipale;
- Legge 24 luglio 2008, n. 125 recante misure urgenti in materia di sicurezza pubblica;
- Legge 23 aprile 2009, n. 38 in materia di sicurezza pubblica e di contrasto alla violenza sessuale; Decreto del Ministero dell'Interno del 5 agosto 2008 in materia di incolumità pubblica e sicurezza urbana:
- Circolari del Ministero dell'Interno n.558/A/421.2/70/456 in data 8 febbraio 2005, n. 558/A421.2/70/195860 in data 6 agosto 2010 e n. 558/SICPART/421.2/70/224632 in data 2.3.2012.

Nella citata nomenclatura normativa ed all'interno del nuovo sistema di lotta alla criminalità che attribuisce ai Comuni un ruolo strategico nel perseguire finalità di

tutela della sicurezza pubblica, l'impianto di videosorveglianza del Comune di Omignano (SA) è senz'altro rivolto a garantire la **sicurezza urbana** che, l'art. 1 del Decreto del Ministero dell'Interno del 5 agosto del 2008,testualmente definisce come il *"bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale."*

La disponibilità tempestiva di immagini presso l'Ente costituisce, inoltre, uno strumento di prevenzione e di razionalizzazione dell'azione della Polizia Locale sul territorio comunale, in stretto raccordo con le altre forze dell'ordine. L'archivio dei dati registrati costituisce, infatti, per il tempo di conservazione stabilito per legge, un patrimonio informativo per finalità di Polizia Giudiziaria, con eventuale informativa nei confronti dell'Autorità Giudiziaria competente a procedere in caso di rilevata commissione di reati.

In particolare, il sistema di videosorveglianza attivato dall'Amministrazione, è finalizzato a:

a) incrementare la sicurezza urbana e la sicurezza pubblica nonché la percezione delle stesse rilevando situazioni di pericolo e consentendo l'intervento degli operatori;
b) prevenire, accertare e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" già richiamato; le informazioni potranno essere condivise con altre forze di Polizia competenti a procedere nei casi di commissione di reati;
c) tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale e gli edifici pubblici e a prevenire eventuali atti di vandalismo o danneggiamento;
d) controllare le aree considerate a maggiore rischio per la sicurezza, l'incolumità e l'ordine pubblico;
e) monitoraggio del traffico e a tutte le attività connesse e strumentali al rilevamento delle infrazioni al codice della strada, con irrogazione delle sanzioni previste;
f) attivare uno strumento operativo di protezione civile sul territorio comunale;
g) acquisire elementi probatori in fattispecie di violazioni amministrative o penali;
h) controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;
i) monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;
j) verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti.

Gli impianti di videosorveglianza non potranno essere e non sono utilizzati , in base all'art. 4 dello Statuto dei Lavoratori (legge 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.
Il citato articolo 4 dello Statuto dei Lavoratori è stato riformato dal c.d. "Jobs Act" (*rectius* dall'art. 23 del decreto legislativo n. 151/2015, in vigore dal 24 settembre 2015, attuativo del c.d. "Jobs Act", ovvero legge delega n. 183/2014, art. 1, comma 7, lett. f), che si riporta testualmente: *«revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore»*). Tale legge che introdotto importanti modifiche rispetto alla possibilità del datore di lavoro di operare un controllo sull'attività lavorativa svolta dai propri dipendenti. A sua volta l'art. 4 comma 1, terzo periodo è stato nuovamente novellato dall'art. 5 c. 2 D.Lgs. n. 185/2016 (in vigore dal 8 ottobre 2016) contente disposizioni correttive ed integrative del D.Lgs. 151/2015. Tutta l'attività di videosorveglianza verrà pertanto svolta in ossequiosa e puntuale adesione a dette normative ed aggiornata ove ne sia mutata la disciplina tempo per tempo.

Gli impianti di videosorveglianza non potranno altresì essere utilizzati per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati o per finalità di promozione turistica.

L'attività di videosorveglianza deve raccogliere solo 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.

La localizzazione delle telecamere e le modalità di ripresa saranno sempre determinate in ossequio ai richiamati principi.

La possibilità di avere in tempo reale dati e immagini costituisce uno strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Locale svolge quotidianamente nell'ambito delle proprie competenze istituzionali; attraverso tali strumenti si perseguono finalità di tutela della popolazione e del patrimonio 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.

L'uso dei dati personali nell'ambito definito dal presente Regolamento, non necessita del consenso degli interessati in quanto viene effettuato per l'esecuzione di un compito di interesse pubblico o comunque

connesso all'esercizio di pubblici poteri e allo svolgimento di funzioni istituzionali di cui è investito il Comune.

Art. 5 – Caratteristiche tecniche dell'impianto

Il sistema è articolato in due sedi distaccate, la sede principale in Via Europa , 16 in Omignano capoluogo, la seconda in Via Nazionale snc in Omignano Scalo

Quanto alla sede principale :

L'architettura software del sistema, realizzata anche per mezzo di un server interno al Sistema del tipo "IBM Thinkpad ST" (in apposita stanza chiusa al pubblico ,) è del tipo P2P (Peer to Peer) (rete paritaria/paritetica), specifica rete informatica con nodi non gerarchizzati unicamente sotto forma di *client o server fissi*, ma sotto forma di *nodi equivalenti* o *'paritari'* (*peer*), potendo fungere al contempo da client e server verso gli altri nodi terminali (*host*) della rete. Mediante questa specifica configurazione adottata dall'Ente, qualsiasi nodo è in grado di avviare o completare una transazione dati in sicurezza. L'Hosting con relativo sistema per data breach e recovery disaster è gestito dalla PA digitale per parte ASP ed Halley Informatica – Matelica – Campania in qualità di sottogruppo- con contratto di servizi già a suo tempo stipulato ed in corso di validità inerente il sistema firewall Fire Box numero 259428 Si precisa che il Server Hosting locale, di proprietà dell'Ente è individuato come segue : " HP" con matricola numero CZ14190011 e processore matematico CORE T3, munito di gruppo di continuità Metasistem. In ogni caso il sistema non permette la perdita di dati sistematica. Il sistema tracciabile si compone di dieci macchine fisse e cinque stampanti di rete in aree inaccessibili al pubblico. Tutte le macchine con pwd alfanumeriche. Le aree di stampa comuni sono multiple, poste in zone ben discrete. Si precisa che i nodi equivalenti possono anche differire nella configurazione locale, velocità di elaborazione, ampiezza di banda e quantità di dati memorizzati, utilizzando il *file sharing e garantendo* un insieme di funzionalità minime ricomprendenti:

- supporto multipiattaforma, *multiserver*, multicanale: con programmi compatibili con tutti i sistemi operativi, server e dispositivi *hardware* fissi
- supporto protocollo IPv6
- *download* dello stesso *file* da più reti contemporaneamente
- offuscamento dell'ID di rete come da protocollo AGID cybersecurity
- offuscamento del protocollo P2P AGID cybersecurity
- supporto proxy e Tor
- supporto crittografia SSL ed SSQL
- gestione da remoto, sia da PC/*notebook*

L'architettura del Sistema informativo virtuale, ai fini del Recovery Disaster AGID compatibile si compone di una rete privata dati cablata, senza dorsali di servizio e con backup proprio e con funzione di data center esterno. Il Sistema informativo è strutturato come segue: un server unico inbounder servizi Active directory e relativi servizi associati. I collegamenti internet avvengono attraverso la rete internet con una

connettività ADSL di esercizio gestita dal Firewal lWindows seriale senza impiego di VPN. Wifi abilitata ed attivabile da interno, anche per VDS con controllo; cablaggio disponibile per accesso fisico con disabilitazione protocollo SSID e TKIP innestato su chiave WEP . Il fornitore dei servizi Hosting e wifi dati è Convergenze spa, già identificato responsabile del trattamento con atto separato a parte.
Il Datacenter è protetto contro il rischio di mancanza dell'energia elettrica da idoneo gruppo di continuità o similare come stabilito dal Recovery Disaster tenuto da PA Digitale di cui in precedenza.

Quanto alla sede secondaria :

L'architettura software del sistema, realizzata anche per mezzo di un server interno al Sistema del tipo "IBM Thinkpad ST" (in apposita stanza chiusa al pubblico ,) è del tipo P2P (Peer to Peer) (rete paritaria/paritetica), specifica rete informatica con nodi non gerarchizzati unicamente sotto forma di *client o server fissi*, ma sotto forma di *nodi equivalenti* o *'paritari'* (*peer*), potendo fungere al contempo da client e server verso gli altri nodi terminali (*host*) della rete. Mediante questa specifica configurazione adottata dall'Ente, qualsiasi nodo è in grado di avviare o completare una transazione dati in sicurezza. L'Hosting con relativo sistema per data breach e recovery disaster è gestito dalla PA Digitale per parte ASP ed Halley Informatica – Matelica – Campania in qualità di sottogruppo- con contratto di servizi già a suo tempo stipulato ed in corso di validità inerente il sistema firewall Fire Box numero 259428 YLHV 00582 Si precisa che il Server Hosting locale, di proprietà dell'Ente è individuato come segue : " Mitrotik" e processore matematico CORE T3, munito di gruppo di continuità batteria zenith. In ogni caso il sistema non permette la perdita di dati sistematica. Il sistema tracciabile si compone di due macchine fisse e una stampante di rete in aree inaccessibili al pubblico. Tutte le macchine con pwd alfanumeriche. L' area di stampa è unica, posta in zone ben discrete. Si precisa che i nodi equivalenti possono anche differire nella configurazione locale, velocità di elaborazione, ampiezza di banda e quantità di dati memorizzati, utilizzando il *file sharing e garantendo* un insieme di funzionalità minime ricomprendenti:

- supporto multipiattaforma, *multiserver*, multicanale: con programmi compatibili con tutti i sistemi operativi, server e dispositivi *hardware* fissi
- supporto protocollo IPv6
- *download* dello stesso *file* da più reti contemporaneamente
- offuscamento dell'ID di rete come da protocollo AGID cybersecurity
- offuscamento del protocollo P2P AGID cybersecurity
- supporto proxy e Tor
- supporto crittografia SSL ed SSQL
- gestione da remoto, sia da PC/*notebook*

L'architettura del Sistema informativo virtuale, ai fini del Recovery Disaster AGID compatibile si compone di una rete privata dati cablata, senza dorsali di servizio e con backup proprio e con funzione di data center esterno. Il Sistema informativo è strutturato come segue: un server unico inbounder servizi Active directory e relativi

servizi associati. I collegamenti internet avvengono attraverso la rete internet con una connettività ADSL di esercizio gestita dal Firewall Windows seriale senza impiego di VPN. Wifi abilitata ed attivabile da interno, anche per VDS con controllo; cablaggio disponibile per accesso fisico con disabilitazione protocollo SSID e TKIP innestato su chiave WEP . Il fornitore dei servizi Hosting e wifi dati è Convergenze spa, già identificato responsabile del trattamento con atto separato a parte.
Il Datacenter è protetto contro il rischio di mancanza dell'energia elettrica da idoneo gruppo di continuità o similare come stabilito dal Recovery Disaster tenuto da PA Digitale di cui in precedenza.

Art. 6 – Informativa

Gli interessati devono 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 l'Ente utilizzerà lo stesso modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita, riportato in *fac-simile* nell'**allegato n. 1** al già richiamato Provvedimento in materia di videosorveglianza del Garante per la Protezione dei dati Personali del **08/04/2010** e di seguito richiamato:

L'Ente, in particolare, si obbliga ad affiggere la richiamata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere, su cui è riportata la seguente dicitura: "Area videosorvegliata – la registrazione è effettuata dal Comune di Omignano , per fini di sicurezza urbana, incolumità e ordine pubblico".

La segnaletica deve essere collocata prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa deve avere un formato ed 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.
In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, andranno installati più cartelli informativi.

L'Ente, nella s.q. di Titolare del trattamento dei dati, si obbliga ad informare la comunità cittadina dell'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, dell'eventuale incremento dimensionale dell'impianto stesso e dell'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, con un anticipo di giorni dieci, mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale.

Art. 7 - Valutazione di Impatto sulla protezione dei dati

In ossequio al disposto di cui all'art. 35, Paragrafo 3, lett. c), RGPD, qualora il trattamento di dati realizzato mediante il sistema di videosorveglianza comunale dia luogo ad una sorveglianza sistematica su larga scala di una zona accessibile al pubblico, l'Ente procederà ad una valutazione di impatto sulla protezione dei dati personali. Di cio' farà menzione il Titolare del Trattamento unitamente al DPO designato nella DPIA di valutazione intermedia gap analysis.
Parimenti si procederà nei casi in cui, il trattamento di dati realizzato mediante il sistema di videosorveglianza presenti un rischio comunque elevato per i diritti e le libertà delle persone fisiche.

In questa fase di prima attuazione della normativa europea, l'Ente, in conformità al disposto di cui all'art. 35, Paragrafi 4 e 5, RGPD, al fine di avere maggiore chiarezza in relazione ai nuovi adempimenti, attenderà ulteriormente la pubblicazione obbligatoria da parte dell'Autorità Garante per la protezione dei dati personali dell'elenco delle tipologie di trattamenti soggetti alla Valutazione di impatto e l'eventuale pubblicazione dell'elenco delle tipologie di trattamenti per le quali non è richiesta una Valutazione di impatto.

Art. 8 - Titolare del Trattamento dei dati (anche "Ente")

Il Titolare del trattamento dei dati è il Comune di Omignano nella persona del sindaco p.t. Dott. Raffaele Mondelli al quale compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personalirilevati attraverso il sistema di videosorveglianza, compresi gli strumenti utilizzati e le misure di sicurezza da adottare.

Il DPO designato, all'adozione del presente regolamento è Micael Polito domiciliato per la carica presso l'Ente.

Il Titolare del trattamento è tenuto a conformare la propria azione al pieno rispetto di quanto prescritto dalle vigenti disposizioni normative in materia e dal presente Regolamento.

Il Titolare del trattamento procede al trattamento dei dati attenendosi alle normative già in precedenza richiamate , vigilando sulla puntuale osservanza delle disposizioni normative e regolamentari.

Il Titolare del trattamento puo' autorizzare al trattamento dei dati eventuali altri soggetti che divengono "**autorizzati al trattamento** ".

Le competenze proprie degli eventuali autorizzati al trattamento dei dati sono analiticamente disciplinate nelle istruzioni , con il quale il Titolare provvede alla loro designazione.

In particolare:

il Titolare del trattamento individuerà e nominerà con propri atti gli autorizzati del trattamento impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29, RGPD; detti autorizzati, all'atto dell'emanazione del presente regolamento, sono già stati opportunamente istruiti e formati da parte del Titolare del trattamento con riferimento alla tutela del diritto alla riservatezza nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati;

il Titolare del trattamento ha già provveduto a rendere l'informativa "*minima*" agli interessati secondo quanto definito al precedente art. 6;

il Titolare del trattamento verifica e controlla che il trattamento dei dati effettuato mediante sistema di videosorveglianza, sia realizzato nel rispetto dei principi di cui all'art. 5 del RGPD e, in particolare, assicura che i dati personali siano trattati in modo lecito, corretto e trasparente; garantisce altresì che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;

il Titolare del trattamento assicura che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

il Titolare del trattamento, tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e, in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, adotta tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del RGPD;

il Titolare del trattamento è coadiuvato dal DPO designato al fine di consentire allo stesso di verificare e poi dare seguito alle eventuali richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del RGPD;

il Titolare del trattamento garantisce il rispetto degli obblighi di sicurezza di cui all'art. 32, RGPD, mettendo in atto misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati,è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie .

il Titolare del trattamento garantisce l'adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso

agli stessi in caso di incidente fisico o tecnico; qualora a ciò non possa provvedere immediatamente e con i mezziassegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti delle Autorità Garanti e Governative;

il Titolare del trattamento assicura l'adozione di procedure volte a testare, verificare e valutare costantemente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento;

il Titolare del trattamento è costantemente assistito dal DPO nelle eventuali procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato ai sensi degli artt. 33 e 34 del RGPD;

il DPO assiste il Titolare del trattamento nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD e del precedente art. 7 del presente Regolamento e nella eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità alla previsione di cui all'art. 36 del RGPD qualora siano previste altre finalità non compatibili con la richiamata normativa istituzionale;

Responsabili del trattamento

Eventuali Responsabili del Trattamento designati (Host, Gestori client ecc.) affiancheranno il Titolare, in conformità alle disposizioni di cui all'art. 30, paragrafo 1, del RGPD, nell'istituzione e aggiornamento del Registro delle attività di trattamento, tenuto in forma scritta, anche in formato elettronico;

il Responsabile del trattamento garantisce che il Responsabile della Protezione dei Dati (DPO) designato dal Titolare del trattamento, sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e si impegna ad assicurargli l'affiancamento necessario per l'esecuzione dei suoi compiti;

il Responsabile del trattamento metterà a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa e per consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto incaricato;

il Responsabile del trattamento è responsabile della custodia e del controllo dei dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta

il Responsabile del trattamento assicurerà che gli autorizzati si attengano, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantisce che vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali;

il Responsabile del trattamento garantisce la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale individuato quale incaricato con riferimento ai trattamenti realizzati mediante l'impianto di videosorveglianza dell'Ente, previo consulto del Responsabile della Protezione dei dati, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;

il Responsabile del trattamento vigila sul rispetto da parte degli incaricati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.

Il Titolare del trattamento è autorizzato a ricorrere a Responsabili esterni del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate che assicurino la tutela dei diritti dell'interessato, **in tutti i casi in cui egli, per la gestione/assistenza delsistema di videosorveglianza, faccia ricorso a soggetti esterni ai quali affidare incarichi, servizi, lavori, forniture o consulenze che comportino un trattamento di dati per conto dell'Ente.**
Inquesti casi, ilTitolare del trattamento procederà a disciplinare i trattamenti da parte del Responsabile esterno mediante contratto ovvero altro atto giuridico che vincoli il Responsabile esterno del trattamento al Titolare del trattamento ai sensi dell'art. 28, RGPD.

Art. 9 – Autorizzati del Trattamento da parte del Responsabile

Il Responsabile del trattamento dei dati procede ad individuare con proprio atto, le persone fisiche incaricate del trattamento dei dati, dell'utilizzazione degli impianti e, nei casi in cui risulta indispensabile per gli scopi perseguiti, della visione delle registrazioni.

L'individuazione è effettuata per iscritto e con modalità tali da consentire una chiara e puntuale definizione dell'ambito del trattamento consentito a ciascun incaricato.

In ogni caso, prima dell'utilizzo degli impianti, gli incaricati dovranno essere istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento e dovranno conformare la propria condotta al pieno rispetto del medesimo.

Gli autorizzati procedono al trattamento attenendosi alle istruzioni impartite dal Responsabile il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.

In particolare, gli autorizzati devono:

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

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

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

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

evitare di creare banche dati nuove senza autorizzazione espressa del Responsabile del trattamento dei dati;

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

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

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

Tra i soggetti designati quali autorizzati i verranno individuati, con l'atto di nomina, le persone cui è affidata la custodia e la conservazione delle chiavi di accesso alla sala operativa ed agli armadi per la conservazione dei supporti magnetici.

Gli Autorizzati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alla istruzione del Titolare o del Responsabile.

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

Art. 10 - Modalità di Raccolta e di Trattamento dei Dati

L'installazione delle telecamere avviene esclusivamente nei luoghi pubblici (strade, piazze, immobili) in conformità all'elenco dei siti di ripresa predisposto dall'Amministrazione Comunale.

L'attività di videosorveglianza deve raccogliere solo dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando solo immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando (quando non strettamente indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti.

Le telecamere di cui al precedente comma 1, consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario.

Il Titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone fisiche che non siano funzionali alle finalità istituzionali dell'impianto attivato. I segnali video delle unità di ripresa saranno inviati presso l'Unita di ricezione, registrazione e visione ubicata nell'Ufficio Polizia Municipale. In questa sede le immagini potranno essere visualizzate su monitor e registrate su supporto magnetico.

I dati personali oggetto di trattamento sono:
- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per le finalità di cui all'art. 4 del presente Regolamento e resi utilizzabili in altre operazioni di trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi;
- raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati.

La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle richiamate disposizioni normative, il termine massimo di durata della conservazione dei dati è limitato ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve specifiche esigenze di ulteriore conservazione.

In ragione di necessità investigative e su richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria il Titolare del trattamento potrà disporre la conservazione delle immagini per un periodo di tempo superiore ai sette giorni previa richiesta al Garante per la protezione dei dati personali che, a seguito di verifica preliminare, potrà rilasciare parere favorevole.

Il sistema di videoregistrazione impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle

informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

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

Art. 11 - Sicurezza dei dati

I dati personali oggetto di trattamento sono conservati ai sensi e per gli effetti del precedente art. 10.

I dati raccolti mediante il sistema di videosorveglianza dovranno essere protetti con idonee e preventive misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato al rischio. Dette misure, in particolare, assicurano:

a) la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
b) il ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico;
c) la sistematica e periodica verifica e valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Ai sensi dell'art. 32, Paragrafo 2, RGPD, nel valutare l'adeguato livello di sicurezza, l'Amministrazione terrà conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati dall'Ente.

A questo fine, sono adottate le seguenti specifiche misure tecniche e organizzative che consentano al Titolare di verificare l'attività espletata da parte di chi accede alle immagini e/o controlla i sistemi di ripresa:

a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi privilegi di visibilità e di trattamento delle immagini. Tenendo conto dello stato dell'arte ed in base alle caratteristiche dei sistemi utilizzati, i soggetti designati quali responsabili e incaricati del trattamento, dovranno essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti a ciascuno, unicamente le operazioni di competenza;
b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, dovrà 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 immagini operazioni di cancellazione o di duplicazione;
c) per quanto riguarda il periodo di conservazione delle immagini, così come già indicato al precedente art. 10, dovranno essere predisposte misure tecniche per

la cancellazione, in forma automatica, delle registrazioni, al rigoroso scadere del termine previsto;

d) nel caso di interventi derivanti da esigenze di manutenzione, si renderà necessario adottare specifiche cautele; in particolare, i soggetti incaricati di procedere a dette operazioni potranno accedere alle immagini oggetto di ripresa solo se ciò si renda indispensabile al fine di effettuare le necessarie verifiche tecniche. Dette verifiche avverranno in presenza dei soggetti dotati di credenziali di autenticazione ed abilitanti alla visione delle immagini;
e) gli apparati di ripresa digitali connessi a reti informatiche dovranno essere protetti contro i rischi di accesso abusivo;
f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza sarà effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie Wi–Fi, WiMax, Gprs).

Come già indicato al precedente art. 8, il titolare del trattamento procede a designare con atto scritto il Responsabile del trattamento dei dati e, quest'ultimo, come già indicato all'art. 9, provvede ad individuare, sempre in forma scritta, le persone fisiche incaricate del trattamento, autorizzate ad accedere ai locali dove sono situate le postazioni di controllo, ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini.

Il Titolare ed il Responsabile del trattamento vigilano sulla condotta tenuta da chiunque agisca sotto la loro autorità e abbia accesso ai dati personali; provvedono altresì ad istruire e formare gli incaricati sulle finalità e sulle modalità del trattamento, sul corretto utilizzo delle procedure di accesso ai sistemi, sugli obblighi di custodia dei dati e, più in generale, su tutti gli aspetti aventi incidenza sui diritti dei soggetti interessati.

Art. 12 – Accesso ai dati

L'accesso ai dati registrati al fine del loro riesame, nel rigoroso arco temporale previsto per la conservazione, è consentito solamente in caso di effettiva necessità per il conseguimento delle finalità di cui all'art. 4 del presente Regolamento.

L'accesso alle immagini è consentito esclusivamente:

a) al Titolare, al Responsabile ed agli incaricati del trattamento;
b) alle Forze di Polizia (sulla base di richiesta scritta formulata dal rispettivo comando di appartenenza e acquisita dall'Ente) nonché per finalità di indagine dell'Autorità Giudiziaria (sulla base di formale richiesta proveniente dal Pubblico Ministero e acquisita dall'Ente);
c) alla società fornitrice dell'impianto ovvero al soggetto incaricato della manutenzione nei limiti strettamente necessari alle specifiche esigenze di funzionamento e manutenzione dell'impianto medesimo ovvero, in casi del

tutto eccezionali, all'amministratore informatico del sistema comunale (preventivamente individuato quale incaricato del trattamento dei dati);

d) all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso alle immagini, previo accoglimento della relativa richiesta, secondo la procedura descritta al successivo art. 13. L'accesso da parte dell'interessato, sarà limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, dovrà pertanto essere utilizzata, da parte del responsabile del trattamento, una schermatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti;

e) ai soggetti legittimati all'accesso ai sensi e per gli effetti degli artt. 22 e ss. L. 241/90 e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'art. 24, comma 7, L. 241/90, l'accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente. L'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante.

Art. 13 - Diritti dell'interessato

In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., RGPD, su presentazione di apposita istanza, ha diritto:

a) di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;

b) ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;

c) di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 RGPD, 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;

d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al
trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21, RGPD.

L'istanza per l'esercizio dei diritti dell'interessato è presentata al Responsabile della Protezione dei dati dell'Ente, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sulla home page del sito istituzionale dell'Ente alla Sezione "Privacy") ovvero al Responsabile del trattamento dei dati individuato eventualmente.

Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:

1. il luogo, la data e la fascia oraria della possibile ripresa;
2. l'abbigliamento indossato al momento della possibile ripresa;
3. gli eventuali accessori in uso al momento della possibile ripresa;
4. l'eventuale presenza di accompagnatori al momento della possibile ripresa; l'eventuale attività svolta al momento della possibile ripresa;
5. eventuali ulteriori elementi utili all'identificazione dell'interessato.

Il responsabile della protezione dei dati dell'Ente ovvero il responsabile del trattamento accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.
Qualora, ai sensi dell'art. 15, paragrafo 3, RGPD, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15, paragrafo 4, RGPD.

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.
Nell'esercizio dei diritti di cui al comma 1 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.

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.

Art. 14 – Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss, RGPD ed alle previsioni che saranno contenute nel Decreto Legislativo di prossima emanazione recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la Direttiva

95/46/CE", in attuazione della delega al Governo di cui all'art. 13, L. 163/2017, noncè il Dlgs. 101/2018.

Art. 15 – Provvedimenti attuativi

Compete alla Giunta Comunale l'assunzione dei provvedimenti attuativi conseguenti al presente Regolamento , in particolare la predisposizione dell'elenco dei siti di ripresa, la fissazione degli orari delle registrazioni, nonché la definizione di ogni ulteriore e specifica disposizione ritenuta utile, in coerenza con gli indirizzi stabiliti dal presente Regolamento se non già disposti , anche con atti separati precedenti.

Art. 16 - Diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali

Chiunque subisca un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento ai sensi delle disposizioni di cui all'art. 82, RGPD.

Il titolare o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79,paragrafo 2,RGPD.

Art. 17 - Pubblicità del Regolamento

Copia del presente Regolamento sarà pubblicata all'albo pretorio e potrà essere reperita anche sul sito internet del Comune.

Art. 18 – Entrata in vigore

Il presente Regolamento entrerà in vigore con il conseguimento della esecutività o della dichiarazione di immediata eseguibilità della deliberazione di approvazione, secondo le leggi vigenti ed osservate le procedure dalle stesse stabilite.
Il presente regolamento abroga ogni disposizione regolamentare precedente che dovesse disciplinare tale materia.

COMUNE DI OMIGNANO (SA)

Allegato 1

RICOGNIZIONE POSTAZIONI DI VIDEOSORVEGLIANZA PER LA SICUREZZA CITTADINA*

Numero venticinque (25) app. VDS di cui numero 2 RAS (lettura targhe) individuate sul territorio in base alle diverse caratteristiche stabilite tempo per tempo anche con il supporto del relativo ufficio tecnico area edilizia pubblica