Città di Afragola

Città Metropolitana di Napoli

REGOLAMENTO

PER LA DISCIPLINA DELLA

VIDEOSORVEGLIANZA DEL COMUNE

DI AFRAGOLA - TERRITORIO

V.1 Delibera di Consiglio Comunale n.

PREMESSE

L'impianto di videosorveglianza installato sul territorio del Comune di Afragola è deputato:

- alla videosorveglianza, interessata alla ricostruzione di eventi, collegati alla commissione di reati o comunque di condotte illecite, o di comportamenti non consoni al rispetto del decoro urbano e della convivenza civile;
- al controllo dei reati ambientali tramite fototrappole ed altri dispositivi mobili;
- alla rilevazione di statistiche da incrociare con altri dati forniti da sensoristica;
- colonnine SOS con video/audio.

In considerazione della natura "integrata" del sistema di videosorveglianza e videocontrollo, per le ragioni predette, il presente Regolamento disciplina i soli trattamenti di competenza del Comune di Afragola.

CAPO I - PRINCIPI GENERALI

Art. 1 - Oggetto e norme di riferimento

1. Costituisce videosorveglianza quel complesso di strumenti finalizzati alla vigilanza in remoto - che si realizza cioè a distanza mediante dispositivi di ripresa video, captazione di immagini ed eventuale conseguente analisi, collegati a un centro di controllo e coordinamento - installati in luoghi pubblici ed aperti al pubblico.
Qualora le immagini riprese dal sistema rendano le persone identificabili, costituiscono dati personali: in tali casi, la videosorveglianza incide sul diritto delle persone alla propria riservatezza. Il presente Regolamento disciplina le modalità di raccolta, trattamento e conservazione dei dati personali posti in essere dal Comune di Afragola mediante il proprio impianto di videosorveglianza, al fine di proteggere gli stessi facendo crescere la fiducia dei cittadini nel mondo digitale.

2. Per tutto quanto non è dettagliatamente disciplinato nel presente Regolamento, si rinvia:
- al Codice in materia di protezione dei dati personali DL 196/2003 'Testo unico sulla privacy';
- al Decreto del Ministro Interno 5 agosto 2008;
- ai Provvedimento del Garante Privacy in materia di videosorveglianza 29.11.2000, 29.04.2004 e 8.04.2010;
- al novellato Regolamento UE 2016/679 del 27 aprile 2016 (GDPR), e conseguente D.Lgs. 101/2018, relativi alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- alla L. 48/2017 "Disposizioni urgenti in materia di sicurezza delle città";
- al Decreto del Ministro dell'Interno 15 agosto 2017 "Direttiva sui comparti di specialità delle Forze di polizia e sulla razionalizzazione dei presidi di polizia";
- al D.Lgs. 51/2018 che ha recepito la Direttiva Ue 2016/680 (c.d. 'Direttiva Polizia) relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.
- alla circolare del Ministero dell'Interno del 2 marzo 2012 recante "Sistemi di videosorveglianza in ambito comunale";
- alla Direttiva del Ministro dell'Interno 30 aprile 2015 "Nuove linee strategiche per il controllo coordinato del territorio";
- alle circolari del Capo della Polizia del febbraio 2005, agosto 2010 e giugno 2017;

- alle Linee generali delle politiche pubbliche per la sicurezza integrata, adottate in sede di Conferenza Unificata il 24 gennaio 2018.

Art. 2 – Definizioni

1. Ai fini del presente regolamento si intende per:

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

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

c) «**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;

d) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

e) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

f) per **DPIA** (**Data Protection Impact Assessment)**, documento di analisi del rischio e valutazione di impatto di cui all'articolo 35 del Regolamento, obbligatoria nei casi indicati;

g) per '**DPO/RPD (Data Protection Officer/Responsabile della Protezione dei Dati**) il soggetto nominato dal Titolare per tutti i trattamenti e attività previste dall'art. 39 del GDPR;

h) per 'D**esignato/Delegato**' il soggetto interno all'Ente cui è affidata la vigilanza sulla raccolta, registrazione, conservazione ed utilizzo delle immagini rilevate dall'impianto;

i) per "**Amministratore Di Sistema**" la/e persona/e cui è/sono attribuite le credenziali per accedere al server unico dedicato alle immagini della video sorveglianza;

j) per "**Persona Autorizzata al Trattamento**", le persone autorizzate dal dirigente designato a monitorare le immagini, a mettere in atto le misure di sicurezza atte a custodire le strumentazioni ed i supporti di registrazione e, nei casi e con le modalità previste, a trattare le immagini;

k) per "**gestore di sistema**", la/e persona/e incaricata/e di garantire - previa disponibilità delle necessarie risorse economiche - l'efficienza tecnica dell'intero impianto di video sorveglianza e l'acquisto di risorse tecnologiche;

l) per "**sistema**" l'insieme delle apparecchiature tecnologiche ed informatiche che costituiscono l'impianto di video sorveglianza;

m) per "**interessato**", la persona fisica, la persona giuridica, l'Ente o associazione cui si riferiscono i dati personali;

n) 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;

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

p) per "**dato anonimo**", il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
q) per "**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.

Art. 3 - Garanzie

1. Il presente regolamento garantisce che il trattamento dei dati personali, effettuato mediante l'impianto di videosorveglianza installato nel territorio del Comune di Afragola, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone durante il loro passaggio in luoghi pubblici o aperti al pubblico, con particolare riferimento alla riservatezza ed alla tutela dell'identità personale.

2. Il presente regolamento garantisce, altresì, i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento. Il sistema informativo e i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzati mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Art. 4 - Finalità istituzionali dell'impianto e Patti per la sicurezza

1. L'impianto di videosorveglianza comunale, anche in relazione a quanto previsto dal Decreto del Ministro Interno 5 agosto 2008 e dalla legge 18 aprile 2017, n. 48 "Disposizioni urgenti in materia di sicurezza delle città" (c.d. 'riforma Minniti') e dalle linee guida approvate il 26 luglio 2018 dalla Conferenza stato – città ed autonomie locali, è **finalizzato** ad assicurare una maggiore sicurezza urbana ai cittadini sia con la necessaria funzione di prevenzione sia permettendo:

a) di acquisire prove utili per accertare e reprimere:
   - la criminalità diffusa, in particolare quella di tipo predatorio e gli episodi di microcriminalità;
   - gli atti di vandalismo o danneggiamento contro immobili, beni e impianti di proprietà o in gestione dell'Amministrazione Comunale;
   - l'abbandono indiscriminato di rifiuti pericolosi in siti a rischio nei quali siano risultati inefficaci o inattuabili altre misure;
   - roghi tossici;
   - le altre attività illecite di natura amministrativa, a scopo sanzionatorio (riferimento art. 13 c. 1 della L. 689/'81);
   - le infrazioni stradali che siano state accertate mediante strumenti di rilevamento, a funzionamento completamente automatico ed omologati dal competente Ministero, idonei alla lettura OCR delle targhe (con o senza telecamere di contesto come supporto), secondo le specifiche disposizioni tecniche stabilite dal Codice della Strada.

b) di monitorare il traffico (anche al fine di razionalizzare l'azione delle pattuglie di Polizia Locale sul territorio, verificare la dinamica di sinistri eventualmente ripresi dalle immagini ed individuare possibili potenziali situazioni di pericolo per la circolazione veicolare e pedonale);

c) di tutelare in particolare minori e anziani (garantendo loro un più elevato grado di sicurezza in alcune particolari aree della Città);

d) di supportare le attività istituzionali dell'Ente, compresa quella di protezione civile, con particolare riferimento al monitoraggio degli incendi boschivi e al livello dei corsi d'acqua.

2. L'impianto di videosorveglianza comunale - al fine di divenire reale strumento di prevenzione e di razionalizzazione dell'azione di polizia su tutto il territorio e favorire in ogni modo la collaborazione tra i vari attori per il potenziamento della sicurezza partecipata ed integrata - può essere **connesso direttamente con le centrali operative delle altre Forze di polizia dello Stato e Carabinieri** operanti sul territorio, oltre ai Vigili del Fuoco per quanto riguarda gli interventi proattivi per il disinnesco di focolai d'incendio.

3. L'utilizzo condiviso - con sistematico accesso - del sistema di videosorveglianza da parte delle forze di polizia Statali dovrà essere ratificato, ai sensi delle linee guida del 26 luglio 2018, con un apposito '**Patto per la sicurezza urbana**' tra Sindaco e Prefetto ispirato ad un progetto di gestione integrata della sicurezza con il quale polizia di stato, carabinieri e polizia locale, nel rispetto delle diverse prerogative e sotto il coordinamento della Prefettura, condividano strategie organizzative per ottenere una sempre più efficace azione di contrasto della criminalità: tale Patto potrà essere sottoposto - se ritenuto opportuno - anche all'approvazione del **Comitato Provinciale per l'Ordine e la Sicurezza**.

4. Alla firma del Patto dovrà seguire la stipula di un **Protocollo operativo interforze che regolamenti l'uso della videosorveglianza da parte delle diverse forze di Polizia sulla base delle norme del presente Regolamento**: in particolare, tale atto dovrà prevedere che chiunque interagisca con l'impianto sia un soggetto avente qualifica di ufficiale o agente di polizia giudiziaria ai sensi dell'art. 57 CPP - munito di credenziali individuali di autenticazione - e dovrà soprattutto evidenziare gli obblighi di protezione dei dati e le connesse responsabilità da parte di ogni forza di polizia partecipante al Protocollo.

5. Le sopra dette finalità istituzionali dell'impianto di videosorveglianza comunale sono conformi alle funzioni istituzionali dell'Ente, in particolare a quelle demandate dal D.lgs.18 agosto 2000 n. 267, dalla legge 7 marzo 1986 n. 65 sull'ordinamento della Polizia Locale, dalle leggi regionali sull'ordinamento della polizia locale, dallo statuto comunale e dal regolamento comunale vigente in tema di tutela della privacy.

6. L'impianto di videosorveglianza comunale non può essere utilizzato per effettuare controlli sull'attività lavorativa dei dipendenti dell'Ente, di altre amministrazioni pubbliche o di altri datori di lavoro pubblici o Privati (Statuto dei lavoratori, L. 300/1970), né per irrogare sanzioni al C.d.S. diverse da quelle di cui al comma 1 lett. 'a' del presente articolo.

Art 5 - Caratteristiche tecniche dell'impianto

1. Il trattamento dei dati personali inizia a seguito dell'attivazione e corretto funzionamento dell'impianto di videosorveglianza comunale.

2. L'impianto - sempre implementabile sulla base delle risorse economiche disponibili nel tempo in Bilancio – può essere costituito da:

a) una serie di strumenti di ripresa (telecamere), di tipo sia analogico che digitale, collegati all'impianto centralizzato unico per la registrazione delle immagini tramite rete informatica. Le telecamere, eventualmente anche dotate di brandeggio e zoom, possono essere utilizzate solo per il controllo di quanto si svolga nei luoghi pubblici ed aperti al pubblico, non nelle proprietà private. Possono riprendere solo le immagini, non l'audio, in quanto in tal modo si realizzerebbe una intercettazione ambientale.

b) una serie di strumenti di rilevamento, a funzionamento completamente automatico ed omologati dal competente Ministero, idonei alla lettura targhe OCR (con o senza telecamere di contesto come supporto) - da collocare ai principali varchi viari di ingresso / uscita dalla Città e/o in aree più centrali, in particolare ove siano imposte restrizioni di accesso - muniti di software in grado di verificare in tempo reale i dati e/o la regolarità dei veicoli in transito ed utilizzati ai sensi del Provvedimento del Garante n. 08 del 04.07.2010 (art. 5.3);

c) un impianto di monitoraggio per la visione in diretta delle immagini riprese dalle telecamere ad esso direttamente collegate, ubicato presso la sala operativa della Polizia Locale, Carabinieri e Polizia di Stato o altro locale idoneo nella disponibilità del Comune di Afragola;

d) un dispositivo centralizzato unico per la registrazione e conservazione delle immagini riprese dalle telecamere (server dedicato, accessibile solo con password informatica);

e) strumenti elettronici portatili, di qualsiasi tipologia purché, regolarmente omologati - per la verifica di veicoli non assicurati, con revisione scaduta, per il contrasto agli eccessi di velocità o per altre simili finalità - i quali diano luogo a cattura di immagini;

f) videocamere mobili (c.d. 'fototrappole') utilizzabili in tutto il territorio comunale -

nell'ambito delle attività istituzionali di Polizia Giudiziaria - per il monitoraggio, l'individuazione di attività illecite e la tutela del territorio e del decoro urbano, ove non risulti possibile (o non si riveli efficace) il ricorso a strumenti e sistemi di controllo alternativi.

3. Ove ricorrano specifiche e comprovate necessità di sicurezza degli operatori, può essere valutata l'opportunità di dotarsi ed utilizzare anche ulteriori strumenti - del tipo 'bodycam' e 'dash cam' (ovvero telecamere indossate sopra la divisa o collocate sui veicoli di servizio) - al fine di attivarli in particolari contesti operativi secondo modalità stabilite in apposito disciplinare, sistemi aeromobili a pilotaggio remoto (c.d. droni) sia per l'esecuzione di riprese ai fini di tutela della sicurezza urbana, sia per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, che per finalità di protezione civile. I dispositivi ed il loro utilizzo devono essere conformi alla normativa vigente, con particolare riferimento alla regolamentazione adottata dall'Ente Nazionale per l'Aviazione Civile e al Codice della Navigazione.

4. L'impianto di videosorveglianza non è connesso con altri sistemi, archivi o banche dati del Sistema Informativo comunale. La tecnologia dell'Impianto di Sorveglianza viene utilizzata però, nell'ambito del progetto "Afragola Città Intelligente", per ricavare dati prettamente numerici e del tutto anonimi utilizzati per migliorare i servizi pubblici. In nessun caso vengono divulgati dati testuali, immagini.

5. Nei limiti previsti dalle norme in vigore, possono essere valutate proposte di integrazione del sistema di videosorveglianza comunale con sistemi privati. Ove tali proposte fossero di interesse, le immagini dovranno essere messe a disposizione dell'Ente a titolo gratuito e senza alcuna ingerenza sulle stesse: i privati interessati dovranno inoltre provvedere ad acquistare a loro spese le attrezzature atte a garantire la connessione al sistema, tenuto conto delle caratteristiche dell'impianto pubblico.

CAPO II - SOGGETTI INTERESSATI E RELATIVI OBBLIGHI E COMPETENZE

Art. 6 – Titolare e Responsabile della Protezione dei dati (DPO)

1. Il Sindaco pro tempore, quale legale rappresentante del Comune di Afragola, è '**Titolare del trattamento dei dati personali**' ed adempie a tutti i connessi obblighi previsti dalla Legge per tale carica. Lo stesso promuove la responsabilizzazione ('**accountability**') delle politiche dell'Ente relativamente al rispetto delle normative in materia di videosorveglianza e cura l'adozione di approcci che tengano costantemente conto del rischio che il trattamento dei dati può comportare per i diritti degli interessati.

2. Il Titolare - quando il trattamento dei dati possa comportare un rischio elevato per i diritti e la libertà delle persone interessate (in ragione del monitoraggio sistematico dei loro comportamenti o per il gran numero di dati sensibili trattati o per altri fattori) - contestualmente all'avvio di utilizzo delle apparecchiature provvede a far redigere la '**DPIA**' **(Data Protection Impact Assessment)** ovvero l'analisi del rischio con valutazione di impatto di cui all'articolo 35 della Delibera 467/2018 (GDPR): tale obbligo è stato ribadito dal Comitato Europeo per la Protezione dei Dati nelle Linee Guida 3/2019.

3. Il Titolare individua e nomina un Responsabile della Protezione dei dati '**DPO** (**Data protection Officer**, in riferimento agli artt. 37 – 39 del GDPR): lo stesso è un esperto, normalmente esterno all'Ente, munito di comprovate competenze circa norme e procedure in materia di sicurezza urbana integrata, cui va affidata la gestione delle problematiche del trattamento dei dati personali, con particolare riferimento ai connessi rischi e responsabilità. Lo stesso - tra l'altro - ha compiti di raccordo sia tra i diversi soggetti e strutture coinvolti nell'attività di videosorveglianza,

sia tra l'Ente e l'Autorità di Controllo; fornisce consulenza per la redazione della DPIA; si occupa dei 'data breach; funge da punto di contatto per gli interessati, ricevendo le loro richieste per conto del Titolare, istruendole e fornendo loro riscontro; rendiconta al Garante circa eventuali reclami; predispone i necessari progetti di miglioramento ed implementazione tecnologica del sistema.

Art. 7 – Designato/Delegato ed Amministratore di sistema

1. Il Sindaco, quale Titolare del trattamento, individua con apposito Atto:
   a. il '**Designato/Delegato**' al trattamento dei dati personali acquisiti tramite videosorveglianza, normalmente individuato nel Dirigente Comandante della Polizia Locale. Il dirigente designato vigila sulla raccolta, registrazione, conservazione ed utilizzo delle immagini rilevate dall'impianto in relazione al servizio di Polizia Locale ed è anche figura di riferimento per quanto concerne gli aspetti procedimentali, ai sensi degli artt. 4-6 della L. 241/1990;
   b. il '**Designato/Delegato**' della videosorveglianza individua ed istruisce un numero delimitato di soggetti autorizzati (Persone Autorizzate al Trattamento) 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. Saranno altresì individuati diversi livelli di accesso in funzione delle specifiche mansioni attribuite, distinguendo coloro i quali sono unicamente abilitati a visionare le immagini dai soggetti abilitati ad effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, etc.);
   c. con cadenza annuale, il '**Designato/Delegato**', nell'ambito dell'organizzazione del Titolare del trattamento, redige una relazione relativa all'impiego e all'efficacia del sistema di videosorveglianza e di videocontrollo.
   d. l''**Amministratore di sistema**', cioè colui/coloro che ha/hanno le credenziali per le quali non vengono applicati i filtri di profilazione al fine di accedere al server unico dedicato alle immagini della video sorveglianza.

Art. 8 - Gestore di sistema

1. Nel medesimo Atto di cui all'articolo precedente, il Sindaco individua altresì il '**Gestore di sistema**' - normalmente il Responsabile della Transizione digitale/Servizi Informatici comunale - al quale è affidata la gestione tecnica e manutentiva necessaria al funzionamento del sistema. Amministratore e Gestore di sistema possono coincidere nella medesima persona. Può essere nominato "Gestore di sistema" anche il soggetto che ha provveduto all'installazione dell'impianto e/o dei dispositivi di videosorveglianza elencati nel presente regolamento.

2. Il Titolare, tramite proprie verifiche periodiche, vigila sull'osservanza di quanto disposto con tale proprio Atto.

Art. 9 – Persona Autorizzata al Trattamento

1. Successivamente all'emanazione dell'Atto di cui all'art. 7 il '**Designato/Delegato**', nomina un numero adeguato di '**Persone Autorizzate al Trattamento (PAT)**' tra gli appartenenti alla Polizia Locale con qualifica di Ufficiali ed Agenti di Polizia Giudiziaria ai sensi dell'art. 55 del Codice di Procedura Penale: gli stessi si occupano materialmente del monitoraggio quotidiano delle immagini del sistema e di custodire le strumentazioni ed i supporti di registrazione. Il '**Designato/Delegato**' affida inoltre ad alcune PAT il compito di trattare le immagini secondo quanto previsto nel successivo Capo III.

2. Le **fototrappole**, sulla base delle problematiche di servizio evidenziate e delle segnalazioni di controllo pervenute, vengono opportunamente collocate - direttamente dal personale di polizia o tramite apposito personale tecnico di fiducia all'uopo individuato - in prossimità dei siti da

monitorare. Trascorso il lasso temporale stabilito il personale di polizia preposto ritira gli apparecchi dai siti, verifica le immagini e gestisce i relativi dati, avviando le eventuali procedure sanzionatorie di carattere amministrativo e/o penale nei confronti delle persone responsabili di violazioni. Le principali operazioni compiute tramite queste apparecchiature (in particolare: siti monitorati, date di inizio e fine delle riprese, data di prima visione delle immagini dopo il periodo di collocazione nel sito e data di cancellazione delle stesse) vanno sempre annotate su apposito registro, anche informatizzato.
Per evitare, in caso di furto di una fototrappola, la possibile dispersione di dati (c.d. 'data breach') ogni fototrappola, ovvero ogni scheda SD installata, dovrà essere opportunamente criptata.
Possono anche essere utilizzate fototrappole munite di controllo da remoto, gestite direttamente dalla Polizia Locale, anche per il tramite del soggetto installatore, il quale, nel rispetto della vigente normativa di settore e delle misure di sicurezza informatiche, metterà a disposizione del Dirigente designato e degli incaricati le immagini richieste dagli stessi per le finalità di cui all'art. 4.

3. Circa le **body cam, dash cam e droni** che fossero eventualmente in dotazione, è predisposto apposito disciplinare contenente le precise modalità di impiego, al fine di garantire la correttezza del trattamento e l'utilizzabilità delle immagini. In particolare, tale Disciplinare dovrà prevedere le circostanze in cui è ammessa l'attivazione dei dispositivi, i soggetti che autorizzano l'avvio delle riprese, tempi e modalità delle stesse ed i soggetti incaricati del prelievo dei dati; conterrà inoltre le procedure per l'utilizzo delle immagini registrate nonché le metodologie di cancellazione al termine del trattamento. Si farà opportuno riferimento alle indicazioni fornite dall'Autorità al Ministero dell'Interno nel 2014.

Art. 10 – Competenze operative e risorse

1. Compete al Sindaco, Titolare del trattamento dei dati personali ed Ufficiale di Governo - nell'ambito delle finalità stabilite dall'art. 4 comma 1 e tenuto conto degli apparati di rilevamento a disposizione - la precisa individuazione dei siti da sottoporre a videosorveglianza.

2. L'elenco dei siti individuati per la video sorveglianza sarà inserito nel medesimo Atto di cui ai precedenti artt. 7 e 8. Il Titolare potrà sempre - previa modifica del citato Atto - variare l'ubicazione ed il numero dei siti video sorvegliati al variare delle esigenze connesse al raggiungimento delle finalità stabilite dall'art. 4 comma 1, ovvero con riguardo agli apparati a disposizione.

3. Compete al '**Designato/Delegato**' verificare che ogni singola telecamera non riprenda in alcun modo aree private - con indebita intrusione nella privacy dei cittadini - disponendo, in collaborazione con il Gestore di Sistema, le necessarie modifiche all'angolo di visuale e/o allo zoom, ovvero individuando ogni altra possibile soluzione tecnica.

4. Compete al Gestore ed ai suoi collaboratori - previo espletamento delle eventuali necessarie procedure amministrative - mantenere in efficienza con i necessari interventi tecnici l'intero impianto di video sorveglianza ed occuparsi della individuazione, fornitura e posa in opera di nuove ed idonee risorse tecnologiche, anche con l'ausilio di specifiche professionalità esterne.

5. La Giunta comunale nel bilancio annuale può stanziare risorse per l'espletamento delle seguenti attività:
   - garantire il funzionamento del servizio, consentendo la manutenzione in efficienza dell'intero impianto esistente e l'acquisto e posa in opera di nuove risorse tecnologiche, con assegnazione dei relativi Capitoli di Bilancio al Gestore di sistema - Responsabile della Transizione digitale/Servizi Informatici comunale;
   - nominare il 'DPO' (Data protection Officer) e far predisporre la 'DPIA' (Data Protection Impact Assessment).

CAPO III - TRATTAMENTO DEI DATI

Art. 11 - Modalità di trattamento dei dati

1. I dati personali raccolti attraverso le riprese video effettuate da telecamere installate sul territorio comunale sono:
   a) trattati in modo lecito e secondo correttezza;
   b) 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 tenuto conto del lasso temporale stabilito dal comma successivo;
   c) trattati con modalità volte a salvaguardare l'anonimato, atteso che le immagini registrate possono contenere dati di carattere personale.

2. Le immagini videoregistrate sono ordinariamente conservate per un periodo **di 7 (sette) giorni successivi alla rilevazione**: tale termine (nel rispetto del principio di proporzionalità) può essere esteso a 90 giorni (o anche più, se necessario) ove vi siano documentate esigenze di indagine (eventualmente anche supportate da specifiche richieste da parte dell'Autorità Giudiziaria e Prefettizia) ovvero, nel caso dei dispositivi di lettura targhe, ai sensi dell'art. 3 del DPR 250/1999. In tali casi è consentita la possibilità di salvare le sole immagini di interesse su supporti non riscrivibili, da conservare in modo protetto per il periodo strettamente necessario in riferimento alla contestazione, all'eventuale applicazione di sanzioni e la definizione del possibile contenzioso in conformità alla normativa.

3. Ove si renda necessario, per ulteriori particolari finalità, un ordinario allungamento del tempo di conservazione, occorre richiedere una verifica preliminare al Garante nei modi di Legge, evidenziando se l'aumento del tempo di conservazione è a carattere provvisorio o permanente.

4. Il sistema impiegato deve essere programmato in modo da operare, allo scadere del termine previsto, **l'integrale cancellazione automatica delle immagini**, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

5. Relativamente alle immagini registrate dalle videocamere mobili (c.d. 'fototrappole'), i 7 giorni di conservazione decorrono dal giorno in cui le stesse vengono per la prima volta visionate dopo il periodo di collocazione nei siti volta a volta individuati.

6. Relativamente alle immagini registrate dagli apparecchi 'bodycam' ovvero 'dash cam' eventualmente in dotazione, i 7 giorni di conservazione decorrono dal giorno in cui le stesse vengono registrate.

Art. 12 – Finalità e casi in cui è consentito l'accesso alle immagini

1. L'accesso alle immagini registrate è consentito esclusivamente per il conseguimento delle finalità istituzionali di cui all'art. 4 comma 1.

2. I dati registrati possono essere visionati:
   immediatamente sulla base di segnalazioni di atti potenzialmente illeciti rilevati da organi di polizia nell'esercizio delle proprie funzioni sul territorio, ovvero rilevati dalla visione delle immagini trasmesse in diretta, ovvero segnalati al momento per le vie brevi da cittadini;
   a seguito di specifiche istanze scritte:
   - inoltrate da parte dell'Autorità Giudiziaria o dalle forze di polizia dello Stato, per acquisire elementi di prova per proprie indagini;
   - inoltrate da altri organi / autorità espressamente autorizzati da specifiche norme;

- inoltrate dall'organo di polizia stradale che ha proceduto ai rilievi di un sinistro ripreso dall'impianto e in capo al quale è l'istruttoria relativa all'incidente;
- inoltrate dal difensore di persona sottoposta alle indagini, a norma dell'art. 391 quater c.p.p., il quale nell'ambito delle investigazioni difensive, può richiedere ed acquisire copia delle immagini di interesse;
- inoltrate da parte di privati cittadini i quali, dichiarando di aver subito un atto illecito, ricerchino elementi di prova utili all'identificazione dei responsabili.

3. In ogni caso di accoglimento delle richieste di cui al comma precedente, l'incaricato della materiale evasione della richiesta dovrà garantire la correttezza delle operazioni di estrapolazione delle immagini di interesse e di riversamento delle stesse su supporto digitale, procedendo ad anonimizzare ogni dato relativo a persone estranee ai fatti di interesse.

4. Non è in ogni caso mai consentito fornire per le vie brevi a privati cittadini e dipendenti copia delle immagini, né far loro visionare immagini registrate.

5. Per finalità comunicative dell'Amministrazione possono essere utilizzate immagini provenienti dall'impianto di videosorveglianza, previa anonimizzazione di ogni dato che consenta l'identificazione di individui.

Art. 13 - Accesso alle immagini registrate ed al server dedicato

1. I monitor degli impianti di videosorveglianza sono collocati in modo tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate;
2. L'accesso alle immagini da parte del Responsabile della videosorveglianza e delle persone autorizzate al trattamento si limita alle attività oggetto della sorveglianza; eventuali altre informazioni di cui vengano a conoscenza mentre osservano il comportamento di un soggetto ripreso, non devono essere prese in considerazione;
3. Nel caso le immagini siano conservate, i relativi supporti vengono custoditi, per l'intera durata della conservazione, in un armadio (o simile struttura) dotato di serratura, apribile solo dal Responsabile e dagli incaricati;
4. La cancellazione delle immagini sarà garantita mediante gli strumenti e le procedure tecnologiche più avanzate; le operazioni di cancellazione devono essere effettuate esclusivamente sul luogo di lavoro;
5. Nel caso il supporto debba essere sostituito per eccessiva usura, sarà distrutto in modo da renderlo inutilizzabile, in modo che non possano essere recuperati i dati in esso presenti, come da Procedura di dismissione delle apparecchiature elettriche ed elettroniche, adottata dal Comune;
6. L'accesso alle immagini ed ai dati personali è consentito, nei limiti di quanto strettamente necessario:
    - al Responsabile della videosorveglianza ed al personale specificatamente autorizzato;
    - ai preposti alle indagini dell'Autorità Giudiziaria o di Polizia;
    - all'Amministratore di Sistema del Comune di Afragola e alla ditta fornitrice dell'impianto, nei limiti strettamente necessari alle loro specifiche funzioni di manutenzione;
    - al terzo, debitamente autorizzato, in quanto oggetto delle riprese.
7. Nel caso di accesso ai dati del terzo, debitamente autorizzato, questi avrà visione solo delle immagini che lo riguardano direttamente;
8. Tutti gli accessi alla visione saranno documentati mediante file di Log, conservati, in maniera sicura e conforme alle procedure di protezione dati e di sicurezza dell'informazione dell'Ente, l'annotazione in un apposito "registro degli accessi" informatizzato, conservato nell'archivio informatico del Comune e conforme alle misure di Sicurezza dell'Informazione dell'Ente, nel quale sono riportati ad opera degli incaricati:

- la data e l'ora dell'accesso;
- l'identificazione del terzo autorizzato;
- i dati per i quali si è svolto l'accesso;
- gli estremi e la motivazione dell'autorizzazione all'accesso;
- le eventuali osservazioni dell'incaricato;
- la sottoscrizione del medesimo.

Art. 14 - Procedura per l'accesso alle immagini

1. Per accedere ai dati ed alle immagini l'interessato dovrà presentare un'apposita istanza scritta ed adeguatamente motivata diretta al Responsabile del corpo di polizia (o al Titolare del trattamento all'indirizzo e-mail indicato nell'Informativa), corredata altresì dalla fotocopia del proprio documento di identità ai fini della sua corretta identificazione.
2. Le richieste di esercizio dei diritti da parte dei soggetti interessati saranno gestiti in coerenza con la relativa procedura interna (v. Procedura di gestione dell'esercizio dei diritti da parte degli interessati).
3. L'istanza deve altresì indicare a quale impianto di videosorveglianza si fa riferimento ed il giorno e l'ora in cui l'istante potrebbe essere stato oggetto di ripresa: nel caso tali indicazioni manchino, o siano insufficienti a permettere il reperimento delle immagini, di ciò dovrà essere data comunicazione all'interessato richiedente, così come nell'ipotesi in cui le immagini di possibile interesse non siano state oggetto di conservazione.
4. Il Responsabile della videosorveglianza sarà tenuto ad accertare l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui il suddetto potrà visionare le immagini che lo riguardano.
5. Il contributo spese da corrispondere da parte del richiedente a copertura dei costi sostenuti per l'espletamento della pratica è di €80,00.

Art. 15 - Pubblicità dell'impianto

1. I cittadini devono essere sempre informati del fatto che stanno accedendo in una zona videosorvegliata. Il Comune, in ottemperanza a quanto disposto dall'art. 13 del Reg. UE 2016/679, comunica ai cittadini la presenza dell'impianto anzitutto con una **informativa di primo livello** consistente in specifici cartelli affissi in tutti i luoghi in cui sono posizionate le telecamere, realizzati secondo quanto previsto dal Garante Privacy. Il relativo modello è raffigurato nell'**Allegato 1**.

2. I cartelli con l'informativa:
   - devono essere collocati prima del raggio di azione della/e telecamera/e, anche nelle immediate vicinanze e non necessariamente a contatto con gli impianti: ove nello stesso sito fossero presenti più telecamere non sarà necessario un cartello per ogni telecamera;
   - devono avere un posizionamento, un formato ed una visibilità tali da essere chiaramente individuabili in ogni condizione di illuminazione ambientale, in particolare in orario notturno.

3. L'apposizione e la manutenzione di tali cartelli informativi, al pari di tutta la segnaletica stradale, è curata dal competente ufficio.

4. Ove vengano utilizzati strumenti mobili/portatili di cui all'art. 5 comma 2 lett 'e', potrà essere al momento apposto un cartello informativo nel solo caso risulti previsto da specifiche norme.

5. Nei luoghi in cui siano temporaneamente posizionate fototrappole, occorre distinguere:

- se il posizionamento dell'apparecchio è fatto su un'area privata, non è obbligatorio segnalarne la presenza con il cartello informativo, a condizione di essere stati autorizzati (anche verbalmente) dal proprietario dell'area;
- nel caso in cui il posizionamento avvenga su un'area pubblica o privata aperta al pubblico, è necessario esporre il cartello informativo per la durata delle riprese, fatti salvi i casi in cui sussistano finalità di sicurezza o necessità di indagine a tutela dell'ordine e sicurezza pubblica ovvero per prevenzione, accertamento o repressione di reati.

6. I conducenti dei veicoli che transitano in aree dove sono attivi sistemi elettronici di rilevamento automatico di violazioni al Codice della Strada devono essere informati della presenza di strumenti atti al rilevamento di immagini.

7. Sul sito istituzionale dell'Ente è resa inoltre disponibile l'**informativa estesa** ai sensi dell'art. 13 Regolamento UE 2016/679 e dell'art. 10 del dlgs 51/2018, con in aggiunta il testo del presente Regolamento.

Art. 16 - Diritti dell'interessato

1. L'interessato al trattamento è la **persona fisica** a cui si riferiscono i dati personali: in riferimento agli specifici chiarimenti forniti dal GDPR, può essere solo una persona fisica e non una persona giuridica, un ente o un'associazione.

2. Nel rispetto delle prerogative previste dal dlgs 51/2018 e con riferimento agli artt. 15 – 22 e seguenti del Regolamento UE n. 2016/679 l'interessato, con apposita **istanza** motivata presentata al Titolare del trattamento utilizzando il modello in **allegato 2**, può esercitare i **diritti** previsti relativamente a dati che lo riguardino e che possano essere stati trattati dal Titolare (tra cui quelli di informazione, accesso, cancellazione, opposizione, trasformazione in forma anonima, blocco, limitazione, ecc.).

3. L'istanza può essere fatta pervenire direttamente al protocollo comunale, ovvero spedita mediante lettera raccomandata, mail o posta elettronica certificata.

4. Circa ogni istanza il Titolare, con l'eventuale supporto del DPO, vi adempie entro 30 giorni dalla data di ricezione (ovvero fino a 90 giorni - previa comunicazione all'interessato di tale proroga - nel caso in cui ricorra giustificato motivo), comunicandone infine l'effettuato adempimento ovvero il motivato diniego. La risposta all'interessato deve essere concisa e resa con linguaggio semplice e chiaro.

5. Nel caso di esito negativo all'istanza, 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. 17 - Cessazione del trattamento

1. In caso di cessazione, per qualsiasi causa, del trattamento dei dati, l'Ente provvede ad eliminare definitivamente dal dispositivo centralizzato unico per la registrazione e conservazione delle immagini tutti i dati presenti.

CAPO IV - TUTELA AMMINISTRATIVA E GIURISDIZIONALE, NORME FINALI

Art. 18 – Tutela

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli artt. 140-bis e seguenti del D.L. 196/2003, novellato dal D. Lgs. 10 agosto 2018, n. 101, dagli artt. 77 e seguenti del Regolamento 2016/679/UE relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e dagli artt. 37 e seguenti del D.lgs 51/2018 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento di reati o esecuzione di sanzioni penali.

Art. 19 – Sanzioni

1. La mancata osservanza degli obblighi previsti in materia di dati personali è sanzionato ai sensi delle vigenti Leggi nazionali e comunitarie, cui si fa rinvio.

Art. 20 – Disposizioni finali

1. Per quanto non disciplinato dal presente regolamento si fa espresso rinvio alle norme legislative vigenti in materia.

2. Il presente Regolamento, dopo la deliberazione del Consiglio Comunale che lo approva, è pubblicato per quindici giorni all'Albo pretorio ed entra in vigore il giorno successivo all'ultimo di pubblicazione, salvo il caso che venga approvato con immediata eseguibilità.

3. A seguito dell'approvazione, il nuovo testo regolamentare come sopra modificato annulla e sostituisce integralmente quello approvato con Deliberazione della Commissione Straordinaria n.29/2007

ALLEGATO 1: Cartello con informativa di primo livello

Attenzione!
Area Videosorvegliata

Afragola Città Intelligente

La registrazione è effettuata da:
Comune di Afragola
Dettagli di contatto: 0818529111
Informazioni preliminari sul trattamento:
I dati sono trattati ai sensi dell'Art.13 del Reg. UE 679/2016
Finalità del trattamento:
Vigilanza Urbana e Pubblica Sicurezza

Ulteriori Informazioni sono disponibili scansionando il seguente QRcode

All'attenzione del Sig. Sindaco
Titolare del Trattamento dei dati Impianto di Videosorveglianza COMUNE DI AFRAGOLA

ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
(artt. 15-22 del Regolamento UE 2016/679)

Il/La sottoscritto/a……
nato/a a…….. il , esercita con la presente richiesta i seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679:

1. **Accesso ai dati personali**

(art. 15 del Regolamento (UE) 2016/679)

Il sottoscritto *(barrare solo le caselle che interessano)*:

☐ chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;

☐ in caso di conferma, chiede di ottenere l'accesso a tali dati, una copia degli stessi, e tutte le informazioni previste alle lettere da a) a h) dell'art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare;

le finalità del trattamento;

le categorie di dati personali trattate;

i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

l'origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);

l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. **Richiesta di intervento sui dati**

(artt. 16-18 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni *(barrare solo le caselle che interessano)*:

☐ rettificazione e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679);

☐ cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi *(specificare quali)*:

a) ……

……..;

b) ……

……..;

c) ……

……..;

nei casi previsti all'art. 17, paragrafo 2, del Regolamento (UE) 2016/679, l'attestazione che il titolare ha informato altri titolari di trattamento della richiesta dell'interessato di

- ☐ cancellare link, copie o riproduzioni dei suoi dati personali; limitazione del trattamento (art. 18)
- ☐ per i seguenti motivi *(barrare le caselle che interessano)*: contesta l'esattezza dei dati personali;
  - ☐ il trattamento dei dati è illecito;
  - ☐ i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
  - ☐ l'interessato si è opposto al trattamento dei dati ai sensi dell'art. 21, paragrafo 1, del Regolamento (UE) 2016/679.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

3. Portabilità dei dati

(art. 20 del Regolamento (UE) 2016/679)

Con riferimento a tutti i dati personali forniti al titolare, il sottoscritto chiede di *(barrare solo le caselle che interessano)*: ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico;

☐ trasmettere direttamente al seguente diverso titolare del trattamento *(specificare i riferimenti identificativi e di contatto del titolare:*
……..):

☐ tutti i dati personali forniti al
☐ titolare; un sottoinsieme di tali dati.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

4. Opposizione al trattamento

(art. 21, paragrafo 1 del Regolamento (UE) 2016/679)

☐ Il sottoscritto si oppone al trattamento dei suoi dati personali ai sensi dell'art. 6, paragrafo 1, lettera e) o lettera f), per i seguenti motivi legati alla sua situazione particolare (specificare):

_____
_____
_____
_____
_____
_____
_____
_____
_____

5. Opposizione al trattamento per fini di marketing diretto

(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)

☐ Il sottoscritto si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il sottoscritto:

☐ Chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.

☐ Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

Recapito per la risposta:
specificare indirizzo oppure e-mail/PEC:

Eventuali precisazioni
Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

(Luogo e data) (Firma)

Allegato 3

Atto di Delega del Soggetto designato al trattamento dei dati personali eseguito mediante sistemi di videosorveglianza

Il Comune di Afragola, con sede in …….. 1, CAP: ……., …….. (NA), Telefono: +39 ……., Fax: +39 …….., PEC: ……., Partita IVA: …….., Codice Fiscale: ……..0, in persona del Sindaco/Legale rappresentante ……

TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

- VISTO il Regolamento UE 679/2016, ad oggetto: "Regolamento europeo in materia di protezione dei dati personali, di seguito GDPR;

- VISTO il Decreto Legislativo 30 giugno 2003, n. 196, ad oggetto: "Codice in materia di protezione dei dati personali";

- VISTO il D. Lgs. 101/2018, recante: "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";

- Visto l'art. 28 del Regolamento Europeo 679/2016, che recita:

"Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato" (…)

- RILEVATO che l'art. 2-quaterdecies del D. Lgs. n. 101/2018 – "*Attribuzione di funzioni e compiti a soggetti designati"* - sancisce quanto segue:

"1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.
2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta".

Ritenuto che su tali basi il Titolare del Trattamento possa, nell'ambito della propria organizzazione prevedere l'attribuzione di specifici compiti e funzioni, relativi al trattamento dei dati personali, a persone fisiche "*Soggetti designati al trattamento"* i quali, in ragione del loro ruolo, intervengono in maniera strategica e nell'ambito della propria area di competenza per la corretta gestione della privacy;

NOMINA SOGGETTO DESIGNATO AL TRATTAMENTO

Il Dr. _____, il quale nell'ambito di attribuzioni, compiti e funzioni, è scelto per le competenze possedute e individuato quale Soggetto designato al trattamento, per i compiti/le funzioni quale Responsabile per la Videosorveglianza, secondo quanto specificato di seguito.

Il Soggetto designato al trattamento è destinatario altresì di specifiche istruzioni in coerenza con i compiti/le funzioni delegate

TERMINI E DEFINIZIONI – GLOSSARIO E ACRONIMI

Archivio: qualsiasi insieme strutturato di Dati Personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Autorità di Controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR;

Consenso dell'Interessato o **Consenso**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati Personali che lo riguardano siano oggetto di Trattamento;

Dati Biometrici: i Dati Personali ottenuti da un Trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati Genetici: i Dati Personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

Dati Giudiziari: Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza

Dati Particolari: Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare Dati Genetici, Dati Biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

Dati relativi alla Salute: i Dati Personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

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;

Destinatario/i: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di Dati Personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di Dati Personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate Destinatari; il Trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del Trattamento;

DPO o **Data Protection Officer**: è una persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37.1 GDPR dal Titolare o dal Responsabile del Trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR;

GDPR o **Regolamento:** Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679.

Incaricato/i o Persona/e Autorizzata/e: si tratta dei Collaboratori autorizzati al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del GDPR. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende:

- dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori e lavoratori a partita IVA, lavoratori a chiamata, part-time, *job-sharing*, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, nonché consulenti e fornitori della Società e, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti Aziendali o Strumenti Personali, operino sulla Rete Aziendale ovvero siano a conoscenza di informazioni aziendali rilevanti quali, a titolo esemplificativo e non esaustivo:

(a) i Dati Personali di clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura commerciale, finanziaria o di strategia di business; nonché (c) i dati e le informazioni relative ai processi aziendali, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale, la cui tutela prescinde dagli effetti pregiudizievoli che potrebbe comportare la diffusione delle medesime.

Soggetti Designati al trattamento – soggetto cui il Titolare o il Responsabile del trattamento prevedono, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, l'attribuzione di specifici compiti e funzioni connessi al trattamento di dati personali, designandolo espressamente.

Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

Limitazione Di Trattamento: il contrassegno dei Dati Personali conservati con l'obiettivo di limitarne il Trattamento in futuro;

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;

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;

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27 GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del GDPR;

Responsabile del Trattamento o **Responsabile**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'Interessato;

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;

Titolare del Trattamento o **Titolare:** 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 o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Trattamento o **Trattato/Trattati:** 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;

Trattamento Transfrontaliero: a) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un Titolare del Trattamento o Responsabile del Trattamento nell'Unione ove il Titolare o il Responsabile siano stabiliti in più di uno Stato membro; oppure, b) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare o Responsabile nell'Unione, ma che incide o probabilmente incide in modo sostanziale su Interessati in più di uno Stato membro;

Violazione Dei Dati Personali ovvero **Data Breach:** è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque Trattati.

DOVERI E DIRITTI

Il Titolare del trattamento ha l'obbligo di adempiere a quanto prescritto dal GDPR e di assicurare che il trattamento di dati personali svolto, nell'ambito della propria organizzazione e da parte del personale che opera sotto la propria autorità, rispetti i principi sanciti.

A tal fine, il soggetto delegato al trattamento ha il dovere di attenersi alle istruzioni impartite dal Titolare del trattamento, di conformarsi comunque alle prescrizioni della normativa privacy e di applicare le adeguate misure di sicurezza organizzative e tecniche previste.

Il Soggetto Designato al trattamento risponde direttamente in caso di eventuali violazioni derivanti da una sua condotta illecita o scorretta o in contrasto con i principi del Regolamento o con le istruzioni impartite dal Titolare, come di seguito definite.

ISTRUZIONI PER IL DELEGATO

Il Soggetto designato al trattamento si impegna ad impartire ai propri collaboratori autorizzati al trattamento, istruzioni documentate in merito alle operazioni di trattamento dei dati personali ed a vigilare sulla loro puntuale applicazione.

Il Soggetto Designato al trattamento dovrà garantire alla specifica categoria di interessati i diritti previsti dal Regolamento 2016/679 e i diritti di informazione previsti dalle norme che disciplinano la materia di riferimento.

A tal fine il Soggetto designato al trattamento provvederà:

a) alla verifica ed adeguamento dei necessari adempimenti privacy, nonché del rispetto dei principi del trattamento ex art. 5 del Regolamento Europeo 2016/679;

b) alla nomina per iscritto degli eventuali incaricati al trattamento, comunicando al Titolare l'elenco degli stessi;

c) a dare istruzioni ed adeguata formazione agli incaricati per il corretto trattamento dei dati personali;

d) a verificare che siano attuate le misure di sicurezza, al fine di ridurre i rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme;

e) all'istituzione e tenuta del registro di accesso alle immagini;

f) alla stesura di una relazione annuale, relativa all'impiego e all'efficacia del sistema di videosorveglianza;

g) a collaborare per la gestione delle richieste di esercizio dei diritti da parte dei soggetti interessati, come previsti dagli artt. 15-22 del GDPR, laddove applicabili o tecnicamente possibili e in coerenza con la relativa procedura interna (v. Procedura di gestione dell'esercizio dei diritti da parte degli interessati);

h) a coadiuvare il Titolare del Trattamento all'implementazione della DPIA.

Il soggetto designato al trattamento dei dati personali eseguito mediante sistemi di videosorveglianza dovrà in generale attenersi ai principi e alle disposizioni previste dal Regolamento aziendale per la videosorveglianza e a coordinare le attività secondo quanto ivi disciplinato.

Nel solo caso di assenza dal servizio per ferie o malattia da parte del Soggetto Designato al trattamento dei dati personali eseguito con sistemi di videosorveglianza, è consentito il ricorso alla delega delle suddette

funzioni a ……..

Inoltre, qualsiasi variazione della situazione oggettiva o delle caratteristiche soggettive del Responsabile, tali da compromettere il corretto espletamento dei compiti descritti, deve essere preventivamente comunicata al Titolare, che potrà in piena autonomia e libertà di valutazione esercitare il diritto di recesso, senza penali ed eccezioni di sorta.

Il Titolare si riserva di revocare, in autonomia e libertà di valutazione, la nomina a Responsabile dei dati trattati nel caso in cui il Responsabile del trattamento non si attenga a quanto indicato con il presente atto di nomina.

TERMINE DELLA PRESTAZIONE

La presente designazione è strettamente correlata all'incarico conferito, ha la medesima durata e non è delegabile.

Una copia del presente atto di designazione viene restituita al Titolare, debitamente firmata per accettazione.

Afragola (NA), lì _____

IL SOGGETTO DESIGNATO AL TRATTAMENTO
(Dr. _____)

IL SINDACO
(Dr. _____)

Allegato 4: Nomina amministratore di sistema personale dipendente

NOMINA AMMINISTRATORE DI SISTEMA
PERSONALE DIPENDENTE

IL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

L'Ente ……, in persona del Legale rappresentante o suo delegato ……,

- **Visto il provvedimento del Garante per la protezione dei dati personali del 27/11/2008**, pubblicato nella G.U. n°300 del 24/12/2008 e s.m.i., nel quale è richiamata l'attenzione dei Titolari del trattamento sulla rilevanza, specificità e particolare criticità del ruolo svolto dall'Amministratore di Sistema, richiedendo l'adozione di adeguate cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, soprattutto quelli realizzati con abuso della qualità di Amministratore di sistema;
- **VISTO il Regolamento UE 679/2016,** ad oggetto: "Regolamento europeo in materia di protezione dei dati personali, di seguito GDPR;
- **VISTO il Decreto Legislativo 30 giugno 2003, n. 196,** ad oggetto: "Codice in materia di protezione dei dati personali";
- **VISTO il D. Lgs. 101/2018,** recante: "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";
- **Considerato** che per l'attribuzione delle funzioni di Amministratore di Sistema occorre indicare l'elencazione analitica degli ambiti di operatività allo stesso consentiti in base al profilo di autorizzazione assegnato;
- **Dato atto che per le necessità organizzative aziendali sono stati definiti i seguenti ambiti di operatività:**
  - Gestione, sicurezza e manutenzione del sistema informatico;
  - Gestione sistemistica delle postazioni di lavoro;
  - Gestione sistemistica, sicurezza e monitoraggio della rete informatica;
  - Gestione sistemistica dei Server aziendali;
  - Back-up e Disaster Recovery;
  - Gestione dei sistemi software e delle basi dati relative agli applicativi in uso;
  - Altro _____;
- **Valutate** la capacità e l'affidabilità tecnica sotto il profilo della sicurezza;

con la presente,

NOMINA

il/la ***Sig.*** **_____** ***Matr.*** **_____**
Cod. Fisc. **_____**, quale Amministratore di Sistema (in seguito AdS) della _____ con il seguente ambito di operatività:

- Gestione, sicurezza e manutenzione del sistema informatico;
- Gestione sistemistica e sicurezza delle postazioni di lavoro;
- Gestione sistemistica, sicurezza e monitoraggio della rete informatica;
- Gestione sistemistica e sicurezza dei Server aziendali;
- Back-up e Disaster Recovery;
- Gestione dei sistemi software e delle basi dati relative agli applicativi in uso;
- Altro _____.

COMPITI E RESPONSABILITÀ DELL'AMMINISTRATORE DI SISTEMA

L'Amministratore di Sistema deve assicurare il corretto funzionamento ed utilizzo del sistema informatico oggetto dell'incarico ed espletare tutte le attività tecniche necessarie, ivi comprese le seguenti:

o progettazione, installazione, configurazione, gestione e manutenzione dei sistemi informatici;
o controllo sul corretto utilizzo, funzionamento e protezione dei sistemi di gestione ed elaborazione dei dati;
o impostazione e gestione dei sistemi di autenticazione e di autorizzazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
o organizzazione e gestione dei flussi di rete;
o gestione dei supporti di memorizzazione;
o manutenzione dell'hardware;
o classificazione analitica delle banche dati ed impostazione/organizzazione di un sistema complessivo di trattamento informatizzato dei dati personali comuni e particolari, nel rispetto della normativa vigente in materia di protezione dei dati personali;
o gestione, ed eventuale progettazione, dei sistemi di salvataggio (backup), anche automatici, con adozione di adeguate procedure per la custodia delle copie di sicurezza dei dati;
o proposta ed implementazione di adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali (antivirus, firewall, IDS ecc.);
o gestione, ed eventuale progettazione, di sistemi di ripristino dei dati e dei sistemi (recovery), anche automatici, che assicurino di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
o adozione di un sistema idoneo alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici; le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Tali registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate ed essere conservate per un congruo periodo, non inferiore a dodici mesi;
○ adozione di tutte le misure di sicurezza adeguate al rischio, ivi comprese:
  ✔ la pseudonimizzazione e la cifratura dei dati personali;
  ✔ la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  ✔ la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  ✔ una procedura per testare, verificare e valutare regolarmente l'efficacia delle
  ✔ misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.
o adozione delle misure di sicurezza ICT emanate dall'AgID, adeguate alla realtà organizzativa aziendale;
o verifica e monitoraggio costante dei sistemi informatici al fine di rilevare immediatamente eventuali tentativi di accessi non autorizzati al sistema provenienti da soggetti terzi, quali accesso abusivo al sistema informatico o telematico, frode, danneggiamento di informazioni, dati e programmi informatici, danneggiamento di sistemi informatici e telematici;
o controllo sugli interventi informatici effettuati da operatori esterni;
o attuazione di un piano di controlli periodici, da eseguire con cadenza almeno semestrale, atti a testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
o provvedere alla distruzione e smaltimento dei supporti informatici di memorizzazione logica obsoleti e/o alla cancellazione dei dati per il loro reimpiego, alla luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento dei dati personali e/o secondo la procedura interna "Procedura di smaltimento apparecchiature elettriche, elettroniche e xxx;
o Redigere una relazione annuale descrittiva delle attività eseguite e delle misure attuate;
o altro _____ .

L' Amministratore di Sistema è tenuto ad un comportamento consapevole, ispirato ai principi di diligenza, fedeltà, correttezza ed idoneo a preservare l'integrità delle risorse aziendali e la riservatezza delle informazioni, nel rispetto degli obblighi del codice civile e della normativa in materia di protezione dei dati personali. E' personalmente responsabile dei dati trattati.

L'accesso ai sistemi informatici è accordato all'AdS unicamente nell'ambito di operatività consentito in base al profilo di autorizzazione assegnato e limitatamente a quanto necessario per garantire il corretto funzionamento e la sicurezza di tali sistemi.

E' fatto espresso divieto di trattare i dati personali per finalità diverse da quelle consentite.

L'AdS è, altresì, tenuto a mantenere l'assoluto riserbo sui dati personali di cui possa venire a conoscenza, anche incidentalmente o per caso fortuito, in ragione dell'esercizio delle funzioni/mansioni assegnate.

Adozione misure di sicurezza

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, l'AdS propone al Titolare l'adozione di misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio, assicurandone la corretta installazione, configurazione, gestione e risoluzione dei problemi nel rispetto dei tempi e delle specifiche fornite.
È responsabilità dell'AdS comprendere le minacce di sicurezza incombenti sui propri sistemi e di adottare le contromisure di sicurezza necessarie ad assicurare confidenzialità, integrità e disponibilità dei dati e delle informazioni.

Analisi dei rischi

Ogni modifica che prevede l'installazione, l'utilizzo, la modifica, l'eliminazione di uno o più sistemi informatici deve essere proposto al Titolare dall'AdS, previa un'adeguata analisi dei rischi che tenga conto delle risorse da proteggere, delle potenziali minacce di sicurezza e dei meccanismi di sicurezza.

Collaborazione con il Titolare, il Soggetto Designato al trattamento ed il Responsabile della Protezione dei Dati

L'AdS è tenuto a collaborare con il Titolare, il Soggetto Designato al trattamento ed il Responsabile della Protezione di Dati, per l'adempimento degli obblighi previsti dal Regolamento Europeo 2016/679.
E' obbligato a collaborare con il Titolare nel condurre, laddove necessario, una valutazione di impatto sulla protezione dei dati (DPIA) ed, in generale, nella predisposizione e/o nell'aggiornamento e/o nell'integrazione di tutti i documenti necessari per il rispetto del Regolamento Europeo in materia di privacy.

Attività di verifica delle misure di sicurezza adottate

L'AdS è responsabile della verifica delle misure di sicurezza adottate e della valutazione della loro efficacia e l'efficienza.
Nel caso in cui, a seguito dell'analisi dei rischi privacy (DPIA) od in conseguenza dell'attività di verifica, le misure di sicurezza adottate risultino non adeguate al rischio, l'AdS deve proporre con urgenza la loro implementazione al Titolare ed ai Responsabili del trattamento.

Data breach

L'AdS è obbligato a reagire agli incidenti di sicurezza prontamente e con spirito di cooperazione ed a segnalare immediatamente eventuali data breach, seguendo le istruzioni dettate dalla **PROCEDURA AZIENDALE DI GESTIONE DELLA VIOLAZIONE DI DATI (DATA BREACH),** pubblicata sul sito internet aziendale nella sezione privacy, cui si fa rinvio.

Documentazione tecnica

L'AdS è responsabile della tenuta ordinata della documentazione e del tempestivo aggiornamento della stessa, in relazione a tutti i sistemi, banche dati, apparati di rete e sicurezza, applicazioni software di qualunque natura e complessità, nonché alle procedure operative di installazione, configurazione ed aggiornamento delle strumentazioni informatiche e telematiche, in relazione al proprio ambito di responsabilità ed operatività. Tale documentazione deve essere messa a disposizione per la consultazione dei soggetti autorizzati.

****

L'Amministratore di Sistema è fin d'ora informato del fatto che il suo operato sarà tracciato con appositi file di log e registrazione e che, con cadenza annuale, il suo profilo sarà oggetto di attività di monitoraggio al fine di verificare la rispondenza alle misure organizzative, tecniche e di sicurezza predisposte per l'esercizio delle funzioni dell'amministratore di sistema, in ottemperanza del Provvedimento del Garante del 27 novembre 2008.

Si informa, infine, l'Amministratore di Sistema che i suoi dati identificativi saranno pubblicati sul sito aziendale, nella sezione privacy, a disposizione di tutti i dipendenti.

La presente designazione di Amministratore di Sistema si dovrà considerare automaticamente revocata in caso di cessazione del rapporto di lavoro.

****

L'Amministratore di Sistema designato, con la sottoscrizione della presente, accetta la presente nomina e

DICHIARA

- di essere a conoscenza degli obblighi previsti dai Provvedimenti del Garante ed in particolare dal provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni del amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)", dalla normativa vigente in materia di trattamento dei dati personali (Regolamento UE 2016/679 e Codice Privacy - D.Lgs. 196/03 novellato dal D.Lgs.101/18 e dai Regolamenti Aziendali, che si impegna a rispettare;
- di garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza e di impegnarsi a procedere al trattamento dei dati personali nel pieno rispetto delle istruzioni del Titolare;
- di possedere le qualità tecniche, professionali e di condotta, le competenze e l'esperienza necessarie allo svolgimento del suddetto incarico.

Afragola (NA), lì _____

IL TITOLARE DEL TRATTAMENTO

IL SOGGETTO NOMINATO AL TRATTAMENTO

Allegato 5: MODELLO DI DESIGNAZIONE PER LE PERSONE AUTORIZZATE AL TRATTAMENTO

Il Comune di Afragola, Città Metropolitana di Napoli , con sede con sede in Piazza Municipio, n. 1, cap 80021, e-mail protocollo@comune.afragola.na.it, tel. 0818529111, sito web: www.comune.afragola.na.it, P.IVA 01547311215, C.F. 80047540630, in qualità di Soggetto designato del trattamento che agisce per delega del Titolare del Trattamento dei dati personali, nella persona del Dott./Dott.ssa _____

DESIGNA

PERSONA AUTORIZZATA AL TRATTAMENTO DEI DATI PERSONALI

Il Sig/Dott._____

in servizio presso _____
(indicare l'eventuale settore/l'Area di appartenenza)

Il quale è in possesso di determinati titoli ed è inquadrato/a secondo le disposizioni legislative e regolamentari specifiche. La Persona autorizzata al trattamento dei dati personali opera nell'ambito delle funzioni di …..…… (inserire la funzione specifica svolta) che è chiamato/a a svolgere attenendosi alle istruzioni impartite e nel rispetto degli obblighi legali di riservatezza.
A tal fine si forniscono informazioni ed istruzioni per l'assolvimento del compito assegnato.

Premesso che:

- il trattamento dei dati deve essere effettuato in modo lecito e corretto e secondo le direttive impartite dal Titolare;
- i dati personali, comuni e particolari devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta, come indicato nell'informativa resa agli interessati (principio di c.d. minimizzazione);
- è necessaria la verifica costante dei dati trattati, il loro aggiornamento, la completezza, la pertinenza e l'integrità degli stessi;
- devono essere applicate le misure di sicurezza tecnico-organizzative ai sensi dell'art. 32 del Regolamento 679/2016 e secondo la Normativa nazionale in vigore in ambito privacy;

In ogni operazione del trattamento l'addetto deve garantire la massima riservatezza ed osservare le seguenti istruzioni a seconda della pertinenza e del ruolo assegnato.

In particolare, il personale autorizzato al trattamento dei dati mediante il sistema di videosorveglianza/fototrappole:

1) dovrà eseguire il trattamento dei dati acquisiti dal sistema di videosorveglianza unicamente per le finalità istituzionali esplicitate nel contratto, nel Regolamento comunale e in ottemperanza alla legislazione vigente;
2) provvederà alla gestione del sistema e dei dati acquisiti, curerà il monitoraggio della funzionalità del sistema e, ove richiesto, all'estrapolazione delle immagini;
3) dovrà vigilare che, durante le operazioni di trattamento, non abbiano accesso ai dati persone prive di autorizzazione;
4) è fatto assoluto divieto di asportare i supporti informatici o cartacei contenenti dati personali di terzi;
5) è vietata la diffusione dei dati;
6) è vietata la comunicazione dei dati laddove non prevista da disposizioni normative e regolamentari;
7) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
8) per l'accesso ai sistemi informatizzati utilizzare password riservata e personalizzata;
9) la password non deve essere composta da riferimenti agevolmente riconducibili alla propria persona (ad esempio nome, cognome, data di nascita, nome del coniuge); non deve essere trascritta su promemoria in vista (ad esempio biglietti dinanzi al pc o affissi in bacheca) o comunicata a terzi;
10) non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento, non

lasciare il PC con l'utenza abilitata per impedirne l'utilizzo fraudolento, non lasciare in vista le informazioni presenti sul monitor. Alla fine del lavoro scollegarsi dal PC;

Per ogni altra misura ed istruzione qui non prevista si richiamano le procedure Aziendali disponibili.

Si ricorda inoltre, che gli obblighi relativi alla riservatezza dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro e che la nomina di Addetto al Trattamento dei dati cesserà automaticamente con il venir meno del rapporto intercorrente tra il Titolare (_____) e la persona autorizzata al trattamento.

Luogo e data _____

Il Soggetto designato	**La Persona Autorizzata al Trattamento**
	per conoscenza e accettazione
_____	_____

Allegato 6: LETTERA DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO ESTERNO

ai sensi del Regolamento Generale sulla Protezione dei Dati UE 2016/679

Il Comune di ……., con sede in ……. n. 1, CAP: ……., ……. (…..), Telefono: +39 ……., Fax: +39 ……., PEC: ……., Partita IVA: ……., Codice Fiscale: ……., in persona del Sindaco/Legale rappresentante …….

TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

VISTO il Regolamento UE 2016/679, ad oggetto: "Regolamento europeo in materia di protezione dei dati personali", di seguito GDPR;

VISTO il Decreto Legislativo 30 giugno 2003, n. 196, ad oggetto: "Codice in materia di protezione dei dati personali", come novellato dal D.Lgs. 101/2018;

PRESO ATTO che:

1. L'art. 4 comma 8 del suddetto Regolamento definisce il Responsabile come: *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".*
2. L'art. 28 del suddetto Regolamento stabilisce che:
   a. comma 1) *"Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato".*
   b. comma 3) "*I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli ii responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento".*
3. VISTA la Determinazione N. …… del …… dell'Area …… relativa all'affidamento del SERVIZIO DI VIDEOSORVEGLIANZA, FORNITURA E MONTAGGIO APPARATI DI VIDEOSORVEGLIANZA" collegato al sistema di Videocamere/fototrappole da installare sul territorio comunale

RICORRE

per l'esecuzione di specifiche attività di trattamento di dati personali riferibili al contratto principale/Affidamento alla società ……., in qualità di Responsabile del trattamento, scelto altresì per le garanzie prestate in materia di protezione dei dati personali.

La società …… con sede legale in Via ……., …
…… Telefono: +39 …….. Fax: +39 ……., email: …….@…..it, PEC:
, PIVA: ……., è pertanto designata Responsabile del trattamento di dati personali, secondo quanto specificato di seguito per **Servizio DI VIDEOSORVEGLIANZA, FORNITURA E MONTAGGIO APPARATI DI VIDEOSORVEGLIANZA" collegato al sistema di Videocamere/fototrappole da installare sul territorio comunale.**

Il Titolare del trattamento autorizza il Responsabile a trattare i dati personali nel rispetto del Regolamento Generale sulla Protezione dei dati UE 2016/679 e secondo quanto disciplinato all'interno del presente atto, per lo svolgimento dei compiti previsti dal contratto principale e dalle disposizioni vigenti disposte dalla

legislazione in materia di settore.

L'ambito e la natura del trattamento autorizzato, le finalità del trattamento da rispettare, le tipologie di dati personali da trattare e le categorie di soggetti interessati coinvolti, nonché tutti gli altri aspetti connessi al trattamento, sono esplicitate nell'Allegato 1.

DOVERI E DIRITTI

Il Titolare del trattamento ha l'obbligo di adempiere a quanto prescritto dal Regolamento UE 2016/679 e di assicurare che il trattamento di dati personali svolto, direttamente o per suo conto dai Responsabili esterni nominati, rispetti i principi sanciti.

Il Titolare del trattamento ha il diritto di vincolare il trattamento dei dati personali svolto dal Responsabile a specifiche istruzioni che lo stesso è tenuto a rispettare.

Il Responsabile, per quanto di propria competenza, è tenuto al rispetto dei Principi applicabili al trattamento di dati personali, ai sensi dell'art. 5 del Regolamento Generale sulla Protezione dei Dati, anche per i propri dipendenti e collaboratori, degli obblighi di riservatezza, integrità e tutela dei dati, nonché a garantire l'utilizzo dei dati stessi esclusivamente per le finalità espresse nel presente documento e nel contratto sottoscritto tra le parti.

Il Responsabile risponde direttamente in caso di eventuali violazioni derivanti da una sua condotta illecita o scorretta o in contrasto con i principi del Regolamento o le istruzioni impartite dal Titolare. A tale scopo, il Responsabile deve collaborare con il Titolare ed assisterlo nei casi in cui l'interessato eserciti i propri diritti, elencati nel Regolamento, adottando opportune misure organizzative e tecniche, nonché nei casi di evento di "data breach" o di necessaria valutazione d'impatto.

Il Responsabile, inoltre, si impegna a mantenere indenne il Titolare del trattamento per qualsiasi sanzione, richiesta e/o danno o spesa, incluse quelle legali, che possano derivare da un mancato rispetto della normativa in materia di protezione dei dati personali allo stesso imputabile, ivi compresi eventuali risarcimenti danni avanzati dai soggetti Interessati, fatto salvo il mancato rispetto della normativa in materia di protezione dei dati personali sia imputabile al Titolare del trattamento ed il Responsabile abbia agito in fede ai requisiti contrattuali.

SICUREZZA DEL TRATTAMENTO

Per i trattamenti operati attraverso la propria organizzazione, il Responsabile, prestatore di servizi, deve garantire l'adozione di un sistema di misure di sicurezza di tipo tecnico ed organizzativo, indicato dal Titolare in quanto ritenuto adeguato rispetto ai trattamenti da effettuare ed ai livelli di rischio presenti secondo i principi espressi all'art. 32 del Regolamento. A tal fine, il Responsabile, in considerazione dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, si impegna a mettere in atto le misure tecniche e organizzative descritte nell'Allegato 2 (MTO) alla presente lettera.

In merito alle misure organizzative da attuare e alle istruzioni da fornire alle Persone autorizzate al trattamento individuate dal Responsabile ai fini del trattamento oggetto della presente nomina si elencano quelle ritenute adeguate dal titolare del trattamento, le quali dovranno essere riportate nell'atto con cui il Responsabile del Trattamento designerà tali soggetti (allegato alla presente nomina Allegato 3):

COMPROVA DELLA CONFORMITÀ

Il Responsabile del Trattamento è tenuto a dimostrare il rispetto dei principi espressi dal Regolamento durante lo svolgimento delle attività di trattamento, inclusa l'adeguatezza e l'efficacia delle misure adottate.

Il Responsabile, se richiesto o necessario, mette a disposizione le informazioni e la documentazione atta a

dimostrare tale conformità, oltre a contribuire in caso di attività di verifica dell'adempimento delle presenti disposizioni svolta da parte del Titolare o dell'Autorità di controllo preposta.

A tal riguardo il Responsabile:

- consente l'accesso alla propria sede o a qualsiasi altro locale ove si svolgono le attività di trattamento dei dati;
- garantisce la possibilità di intervistare i soggetti autorizzati al trattamento;
- permette l'accesso ai sistemi informativi e strumenti informatici ove avvengono le operazioni di trattamento.

NOTIFICA DI VIOLAZIONE

Il Responsabile ha l'obbligo di informare il Titolare nel caso in cui si verifichi una violazione dei dati personali, senza ingiustificato ritardo e, in ogni caso, entro e non oltre 24 ore dal momento in cui ne è venuto a conoscenza. In tal modo il Titolare, opportunamente avvertito, avrà il tempo necessario per notificare la violazione all'autorità di controllo e, ove necessario, agli Interessati.

Il Responsabile, al momento della dichiarazione di violazione, dovrà fornire le seguenti informazioni in merito:

- alla natura della violazione dei dati personali, alle categorie e al numero approssimativo dei soggetti interessati coinvolti;
- alle probabili conseguenze della violazione dei dati personali;
- alle misure adottate o che intende adottare per porre rimedio alla violazione dei dati personali e, eventualmente, per attenuarne i possibili effetti negativi.

Il Responsabile deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono anche previste sanzioni di natura penale.

In ogni caso la responsabilità penale per eventuale uso non corretto dei dati oggetto di tutela, resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.

In merito alla responsabilità civile, si fa rinvio all'art. 154 del Codice, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando, a livello pratico, che, per evitare ogni responsabilità, l'operatore e tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

ISTRUZIONI PER IL RESPONSABILE

Il Responsabile del Trattamento si impegna ad impartire per iscritto, ai propri collaboratori autorizzati al trattamento, istruzioni in merito alle operazioni di trattamento dei dati personali ed a vigilare sulla loro puntuale applicazione in accordo del considerando art. 28 del Regolamento UE 679/2016.

Tutti i dati personali devono essere conservati sotto la esclusiva e diretta responsabilità del Responsabile del Trattamento mediante le attività e le relative procedure descritte nel documento allegato (da redigere ed allegare da parte del fornitore), coordinandosi, se necessario, con l'Ente per l'individuazione e l'applicazione delle necessarie misure di sicurezza atte a garantire la riservatezza ed integrità dei suddetti dati.

Il Responsabile del Trattamento dovrà garantire alla specifica categoria di interessati i diritti previsti dal Regolamento 2016/679 e i diritti di informazione previsti dalle norme che disciplinano la materia di riferimento.

Pertanto:

- i dati devono essere trattati solo per l'erogazione dei servizi espressi all'interno del contratto e/o

secondo quanto stabilito in altri atti documentabili, tra cui la presente lettera. Non è consentito effettuare ulteriori trattamenti che possano differire da tali finalità, salvo che non sia espressamente richiesto dal Titolare del trattamento o derivi da obblighi di legge.

- il Responsabile del trattamento non deve comunicare a terzi o diffondere i dati personali dei soggetti Interessati, se non previa autorizzazione del Titolare del trattamento.
- il Responsabile a tenuto ad adottare tutte le misure adeguate al trattamento, richieste ai sensi dell'articolo 32 del Regolamento e, ove previsto, dal Titolare.
- è onere del Responsabile avvertire il Titolare qualora si configuri un qualsiasi rischio derivante dal trattamento di dati per la gestione dei servizi affidati o ad essi conseguenti.
- il Responsabile si impegna ad individuare gli addetti da destinare al servizio e a designarli quali persone autorizzate al Trattamento, indicando l'ambito di competenza e le specifiche funzioni ad essi attribuiti, mediante compilazione dell'apposito modello (Allegato 4). I nominativi delle persone autorizzate al trattamento dovranno essere riportati nell'elenco di seguito predisposto. Il responsabile aggiornerà l'elenco nei casi di sostituzione e/o aggiunta del personale incaricato.
- Il responsabile manterrà traccia degli accessi eseguiti da parte delle persone autorizzate al trattamento individuate e designate, unitamente alla motivazione e agli estremi dell'autorizzazione all'accesso, mediante apposito registro (REGVS – Allegato 5).
- il Responsabile deve garantire che le persone autorizzate al trattamento dei dati personali sotto la sua autorità si siano impegnate alla riservatezza e siano adeguatamente istruite affinché svolgano il trattamento di dati personali nel rispetto del Regolamento e delle istruzioni impartite dal Titolare.
- il Responsabile a tenuto a collaborare con il Titolare del trattamento, tramite adeguate misure tecniche e organizzative, affinché sia garantito un corretto riscontro in caso di richieste pervenute dagli Interessati per l'esercizio dei propri diritti, ivi compreso il diritto all'oblio e alla portabilità ove applicabili.
- il Responsabile assiste il Titolare nell'adozione di adeguate misure di sicurezza.
- i dati non devono essere conservati per un periodo superiore a quello necessario per le finalità del trattamento, indicato dal Titolare del trattamento o da specifiche normative di settore ove applicabili.
- Il Responsabile deve redigere il registro delle attività di trattamento in conformità ai requisiti previsti all'art. 30, comma 2 del GDPR.

Il Responsabile si impegna ad osservare la massima riservatezza nel trattamento dei dati ed in particolar modo si impegna a rispettare il divieto di comunicazione a terzi e di diffusione dei dati personali trattati; questi rimangono di proprietà del Titolare.

Il Responsabile, per l'esecuzione di specifiche attività, può avvalersi di sub-responsabili al trattamento, previa autorizzazione scritta del Titolare. I Sub-Responsabili del trattamento sono autorizzati a trattare dati personali degli interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti dal Responsabile ed è fatto loro divieto di trattare tali dati personali per altre finalità. I Sub-Responsabili dovranno a loro volta garantire misure tecniche ed organizzative adeguate, atte a soddisfare gli obblighi di protezione dei dati. Il Responsabile dovrà fornire al Titolare l'elenco aggiornato di tutti i sub-responsabili di cui si avvale.

Per le attività in oggetto del servizio si esclude l'eventuale trasferimento di dati personali verso un paese terzo (extra UE) o un'organizzazione internazionale.

Eventuali ulteriori allegati alla presente Nomina, valgono esclusivamente per le parti non in contrasto con

quanto dichiarato nella presente.

TERMINE DELLA PRESTAZIONE

La presente designazione avrà la medesima durata del Contratto. Qualora questo venisse meno o perdesse efficacia e per qualsiasi motivo, anche la presente nomina verrà automaticamente meno senza bisogno di comunicazioni o revoche, ed il Responsabile non sarà più legittimato a trattare i dati qui considerati.

Nella conclusione del servizio oggetto dell'accordo, la presente nomina si intenderà revocata e il Responsabile dovrà consegnare al Titolare, se espressamente richiesto, gli archivi informatici e cartacei contenenti i dati personali oggetto della presente lettera.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali e in aderenza alla specifica materia di riferimento

Una copia del presente atto di nomina viene restituita al Titolare, debitamente firmata per accettazione.

Data

Il Titolare del Trattamento
(Comune di Afragola)

Data

Il Responsabile del trattamento
(……..)

DESCRIZIONE SERVIZIO

I servizi svolti dalla Società **.....** ai sensi del Contratto Principale sono:

- ***Servizio DI VIDEOSORVEGLIANZA, FORNITURA E MONTAGGIO APPARATI DI VIDEOSORVEGLIANZA" collegato al sistema di Videocamere/fototrappole da installare sul territorio comunale***

PARTE II – DESCRIZIONE DEL TRATTAMENTO E TIPOLOGIA DI DATI

Descrizione del trattamento	**Operazioni effettuate (con o senza l'ausilio di processi automatizzati) sui dati personali**	**Finalità del trattamento**	**Durata del trattamento**	**Dati personali trattati**	**Categorie di interessati**
Servizio DI VIDEOSORVEGLIANZA, FORNITURA E MONTAGGIO APPARATI DI VIDEOSORVEGLIANZA" collegato al sistema di Videocamere/fototrappole da installare sul territorio comunale	• **Raccolta** • **Registrazione** • **Organizzazione** • **Strutturazione** • **Conservazione** • **Adattamento o Modifica** • **Estrazione** • **Consultazione** • **Uso** • **Comunicazione** • **Diffusione** • **Raffronto/Interconnessione** • **Cancellazione** • **Distruzione**	Sulla base del seguente principio di liceità: Articolo 6, paragrafo 1, lettera e) (necessità al fine di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri), le finalità perseguite con l'attivazione del sistema di controllo a mezzo videocamere/fototrappole, sono: - Il controllo del rispetto della normativa nazionale, regionale e locale in materia di conferimento e abbandono rifiuti; - La prevenzione igienico sanitaria ed il degrado urbano; - Sicurezza urbana e polizia giudiziaria nell'ambito esclusivo delle attività della Polizia Locale e delle Forze dell'Ordine;	**Come da contratto**	• **Immagini (foto – video)**	• **Utenti/cittadini**

MISURE TECNICHE E ORGANIZZATIVE

Si riportano di seguito i principali requisiti di sicurezza delle informazioni e delle relative misure di sicurezza attuate dal Responsabile

Nell'ambito dell'appalto in oggetto, in conformità a quanto previsto dalle specifiche di gara e di quanto convenuto con i rappresentanti dell'Amministrazione, è stata realizzata la fornitura e posa in opera degli apparati di seguito descritti.

Videocamere

Sono state installate, al momento, n°…… videocamere nei seguenti siti:

- Via …….. 1
- Via ……..
- Via ……..

Per le ulteriori videocamere previste dal progetto, si è in attesa che l'Amministrazione definisca gli esatti siti di interesse.

Le videocamere sono dotate di memoria SD su cui avviene la registrazione dei filmati video delle scene riprese dalle videocamere stesse.

La registrazione avviene in modalità continuativa H24. La durata massima del periodo di retention delle immagini video nella memoria SD delle videocamere è stato definito in 7 giorni, con cancellazione automatica, per sovrascrittura, in modalità FIFO (First In First Out). La durata effettiva, non superiore ai 7 giorni, è funzione della capacità delle schede SD e della qualità video richiesta.

Nelle scene video riprese dalle videocamere è stata configurata un'area "sensibile", di interesse dell'Amministrazione, per cercare di individuare gli atti di deposito abusivo di rifiuti nell'immediatezza della loro esecuzione. Il transito di auto o persone nella suddetta area "sensibile" dà luogo alla generazione di un allarme da parte delle videocamere.

Le videocamere sono collegate, tramite connessione su rete dati mobile, con il Centro di controllo ……..

Per ciascuna telecamera è stata realizzata una connessione protetta, in modalità VPN IPsec site to site, con i firewall dell'infrastruttura IT del Centro …….. Tali connessioni non consentono accessi alle videocamere dalla rete internet pubblica.

Tramite le VPN site to site, le videocamere sono connesse con la piattaforma di centralizzazione video del Centro …….. per il monitoraggio real time della connessione stessa e della diagnostica relativa allo stato funzionale delle videocamere.

Al verificarsi di situazioni di caduta di connessione, di anomalie funzionali o di allarmi di transito nelle aree "sensibili" configurate nelle videocamere, gli operatori ricevono, "real time", una segnalazione di allarme nel sistema integrato di supervisione e monitoraggio del Centro. Solo in tale situazione, gli operatori visualizzeranno le immagini video live delle videocamere, per constatare la situazione che si sta presentando.

In assenza di allarmi (situazione di normalità), nessuno visualizza le immagini video riprese dalle videocamere.

Nella gestione di un evento di allarme, se la situazione riscontrata nella visione delle immagini live è quella di un deposito abusivo di rifiuti, gli operatori del Centro accederanno da remoto agli archivi video presenti sulle schede SD a bordo delle videocamere per estrarre il filmato video relativo all'atto di deposito abusivo ed inviarlo, via mail/trasferimento remoto/spediti su supporto informatico - i file trasmessi saranno sempre protetti da password che verrà trasmessa su canale diverso da quello utilizzato per l'invio (sms/whatsapp), ai referenti definiti dell'Amministrazione. Il filmato video, una volta trasmesso, non viene conservato.

A fronte di richiesta dei referenti dell'Amministrazione, delle FF.OO. o della AA.GG., di filmati video ripresi dalle videocamere, gli operatori procederanno all'estrazione dei filmati dagli archivi a bordo videocamera ed al loro invio. Il filmato video, una volta trasmesso, non sarà conservato.

L'accesso alle immagini video è sempre possibile dal personale del Centro di Controllo a fronte di specifiche segnalazioni di allarme che dovessero pervenire. E' onere dell'Amministrazione richiedere la visualizzazione dei file di log per controllare eventuali accessi non autorizzati.

Fototrappole

Sono state installate, al momento, n°…… fototrappole nei seguenti siti:

- Via …….
- Via …….
- Via …….

Come previsto da progetto, le fototrappole sono dotate di SIM cellulare per l'invio automatico di un allarme al verificarsi del transito di un'auto o di una persona nell'area "sensibile" configurata nella scena video ripresa dalla fotocamera, sulla base delle indicazioni dell'Amministrazione.
L'allarme viene inviato dalla fotocamera stessa, via mail, al Centro operativo, con allegato il filmato video registrato, della durata di 10 sec.
Se nel filmato video gli operatori individuano situazioni di deposito abusivo di rifiuti, trasmettono la mail via mail / trasmissione remota / spediti su supporto informatico - i file trasmessi saranno sempre protetti da password che verrà trasmessa su canale diverso da quello utilizzato per l'invio (sms/whatsapp) ai referenti definiti dell'Amministrazione. In ogni caso, il filmato video, una volta trasmesso, non viene conservato nel Centro operativo
Sulla base delle sopra descritte modalità operative, il Centro operativo non è in possesso in alcun modo, delle immagini video riprese dalle fotocamere installate.
L'accesso alle immagini video è sempre possibile dal personale del Centro di Controllo a fronte di specifiche segnalazioni di allarme che dovessero pervenire. E' onere dell'Amministrazione richiedere la visualizzazione dei file di log per controllare eventuali accessi non autorizzati.

Misure di sicurezza generali adottate

Nell'adottare le misure di sicurezza si è tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

La ……. ha messo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, provvedendo su base permanente alla riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, ha predisposto un sistema per ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico ed ha attivato una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Inoltre nel valutare l'adeguato livello di sicurezza, si è tenuto conto in special modo 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.

Di seguito una sintesi delle misure di sicurezza tecniche ed organizzative adottate, ……..

Misure di sicurezza specifiche – certificazioni aziendali

Sono state inoltre adottate tutte le misure di sicurezza tecniche ed organizzative previste dai percorsi di certificazione secondo le seguenti specifiche tecniche:

1) ABILITAZIONE PER GLI IMPIANTI D.M. 37/08: Lettere A-B-C-D-E-F-G
2) ISO 9001: 2015
3) SOA: OS5 VII (15,5M€); OS19II (0,5M€); OS30V(5,5M€),
   Progettazione e costruzione fino alla VIII classifica illimitata
4) UNI 10891: Attività e classi funzionali incluse nella licenza: B;
   Livelli dimensionali: 1; Ambiti territoriali: 5 (Nazionale)
5) IMQ – CMS:

Certificazione dei centri di monitoraggio e di ricezione di allarme. Tipologia C.
Conformità Norme: UNI CEI EN 50518:2020
Conformità: D.M Interno 1 dicembre 2010, n.269
Conformità: D.M Interno 4 giugno 2014, n.115
Conformità: Disciplinare del Capo della Polizia D.G. Pubblica Sicurezza del 24.02.2015.

6) LICENZA PREFETTIZIA

Istituto di Vigilanza per: Attività e classi funzionali incluse nella licenza: B;
Livelli dimensionali: 1; Ambiti territoriali: 5 (Nazionale)

7) ISO 14001 - Sistemi di gestione ambientale
8) ISO 45001 - Salute e sicurezza sul lavoro

SA 8000 - Certificazione etica
ISO 27001 - Sicurezza delle informazioni
RATING DI LEGALITA' : *** Autorità Garante della Concorrenza e del Mercato .
ECOVADIS: Sustainability Rating & Performance Monitoring - reliable