COMUNE DI CANICATTINI BAGNI

PROVINCIA DI SIRACUSA

REGOLAMENTO COMUNALE SULLA VIDEOSORVEGLIANZA

Allegato alla delibera C.C. n. 25 **del** 31 / 07 / 2023

Sommario

Art.1. Premessa 3

Art.2. Norme di riferimento e principi generali 3

Art.3. Definizioni 4

Art.4 Finalità istituzionali dei sistemi di videosorveglianza 5

Art.5 Caratteristiche tecniche dell'impianto 7

Art.6. Informativa 7

Art.7. Valutazione di Impatto sulla protezione dei dati 8

Art.8 Titolare e Responsabile del Trattamento dei dati 8

Art.9 Incaricati del Trattamento... 8

Art.10 Modalità di Raccolta e di Trattamento dei Dati 9

Art.11 Sicurezza dei dati 10

Art.12 Accesso ai dati 11

Art.13 Utilizzo di telecamere mobili 11

Art. 14 Utilizzo di telecamere modulari 12

Art.15 Diritti dell'interessato 12

Art.16 Tutela amministrativa e giurisdizionale 13

Art.17 Provvedimenti attuativi 13

Art.18 Pubblicità del Regolamento 13

Art.19 Norma di rinvio 13

Art. 20 Entrata in vigore 13

Art. 1 – Premessa

1. Le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto a cui si riferiscono, costituiscono dati personali.
2. La videosorveglianza dà luogo pertanto a trattamento di dati personali e incide sul diritto alla riservatezza delle persone fisiche eventualmente presenti nell'area sottoposta a ripresa.
3. Il presente Regolamento garantisce che il trattamento dei dati personali, effettuato mediante sistemi di videosorveglianza gestiti ed impiegati dal Comune di Canicattini Bagni nel territorio comunale, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

Art. 2 - Norme di riferimento e principi generali

1. Il presente regolamento disciplina il trattamento la raccolta e la conservazione di dati personali, r mediante l'impianto di videosorveglianza cittadina, attivato nel territorio del Comune di Canicattini Bagni.
2. Per tutto quanto non dettagliatamente disciplinato dal presente Regolamento, si rinvia a quanto disposto dal:
   - Regolamento UE Generale sulla Protezione dei Dati 2016/679 (di seguito RGDP) relativo "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";
   - Direttiva UE 2016/680 relativa "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio";
   - DPR n. 15 del 15/01/2018 recante "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia";
   - Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell'8 aprile 2010 (G.U. n. 99 del 29/04/2010);
   - Decreto Ministero dell'Interno 05/08/2008 (GU n. 186 del 09.08.2008);
   - Legge n. 38/2009 recante "misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale nonché in tema di atti persecutori";
   - Linee Guida 3/2019 del Comitato Europeo per la protezione dei dati adottate in data 29/01/2020 (trattamento di dati personali attraverso videosorveglianza).
3. La Videosorveglianza in ambito Comunale si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5, RGDP e, in particolare:

Principio di liceità – Il trattamento di dati personali da parte di soggetti pubblici è lecito allorquando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri

di cui è investito il Titolare del trattamento in ossequio al disposto di cui all'art. 6, Paragrafo 1, lett. e), RGPD. La videosorveglianza comunale pertanto è consentita senza necessità di consenso da parte degli interessati.

Principio di necessità – In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all'art. 5, Paragrafo 1, lett. c), RGPD, il sistema di videosorveglianza, i sistemi informativi ed i programmi informatici utilizzati, sono configurati per ridurre al minimo l'utilizzazione di dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di videosorveglianza.

Inoltre, qualora non sia necessario individuare le persone, i sistemi devono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, con riprese di insieme e, il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati.

Principio di proporzionalità – La raccolta e l'uso delle immagini devono essere proporzionali agli scopi perseguiti.

In applicazione dei principi di proporzionalità e di necessità, nel procedere alla commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un'effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili.

Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi.

La proporzionalità va valutata in ogni fase o modalità del trattamento.

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

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

Art. 3 – Definizioni

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

- per «**trattamento**», qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- per "**banca dati**", il complesso organizzato di dati personali, formatosi attraverso le apparecchiature di registrazione e ripresa video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nelle aree interessate dalle riprese;
- per « **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;
- per "**responsabile del trattamento**" la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- per «**incaricato del trattamento**», la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del titolare o del responsabile del trattamento;
- per "**interessato**", la persona fisica cui si riferiscono i dati personali oggetto di trattamento;
- per «**terzo**», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- per «**violazione dei dati personali**», la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Art. 4 – Finalità istituzionali dei sistemi di videosorveglianza

1. Le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza attengono allo svolgimento delle funzioni istituzionali proprie dell'amministrazione comunale in conformità a quanto previsto dal:
   - D.lgs. 18 agosto 2000, n. 267 – TUEL;
   - D.P.R. 24 luglio 1977, n.616;
   - D.lgs. 31 marzo 1998, n. 112;
   - Legge 7 marzo 1986, n. 65, sull'ordinamento della Polizia Municipale;
   - Legge 24 luglio 2008, n. 125 recante misure urgenti in materia di sicurezza pubblica;
   - Legge 23 aprile 2009, n. 38 in materia di sicurezza pubblica e di contrasto alla violenza sessuale;
   - Decreto del Ministero dell'Interno del 5 agosto 2008 in materia di incolumità pubblica e sicurezza urbana;
   - Circolari del Ministero dell'Interno n.558/A/421.2/70/456 del 8 febbraio 2005, n.558/A421.2/70/195860 del 6 agosto 2010 e n. 558/SICPART/421.2/70/224632 del 2 marzo 2012.

2. Nella richiamata cornice normativa e all'interno del nuovo sistema di lotta alla criminalità che attribuisce ai Comuni un ruolo strategico nel perseguire finalità di tutela della sicurezza pubblica, l'impianto di videosorveglianza del Comune di Canicattini bagni è precipuamente rivolto a garantire la **sicurezza urbana** che, l'art. 1 del Decreto del Ministero dell'Interno del 5 agosto del 2008,

testualmente definisce come il "*bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale.*"

3. La disponibilità tempestiva di immagini presso il Comune costituisce, inoltre, uno strumento di prevenzione e di razionalizzazione dell'azione della Polizia Municipale sul territorio, in stretto raccordo con le altre forze dell'ordine.
4. L'archivio dei dati registrati costituisce, infatti, per il tempo di conservazione stabilito per legge, un patrimonio informativo per finalità di Polizia Giudiziaria, con eventuale informativa nei confronti dell'Autorità Giudiziaria competente a procedere in caso di rilevata commissione di reati.
5. In particolare, il sistema di videosorveglianza attivato dall'Amministrazione, è finalizzato a:
   a) incrementare la sicurezza urbana e la sicurezza pubblica nonché la percezione delle stesse rilevando situazioni di pericolo e consentendo l'intervento degli operatori;
   b) prevenire, accertare e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" già richiamato; le informazioni potranno essere condivise con altre forze di Polizia competenti a procedere nei casi di commissione di reati;
   c) tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale e gli edifici pubblici e a prevenire eventuali atti di vandalismo o danneggiamento;
   d) al monitoraggio del traffico;
   e) attivare uno strumento operativo di protezione civile sul territorio comunale;
   f) ad acquisire elementi probatori in fattispecie di violazioni amministrative o penali;
   g) per controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;
   h) monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;
   i) verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti.
6. Gli impianti di videosorveglianza non potranno essere utilizzati, in base all'art. 4 dello statuto dei lavoratori (legge 300 del 20 maggio 1970) e ss.mm.ii. per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.
7. Gli impianti di videosorveglianza non potranno altresì essere utilizzati per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati o per finalità di promozione turistica.
8. L'attività di videosorveglianza deve raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando (quando non indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza.
9. La localizzazione delle telecamere e le modalità di ripresa saranno sempre determinate in ossequio ai richiamati principi.
10. La possibilità di avere in tempo reale dati e immagini costituisce uno strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Municipale svolge quotidianamente nell'ambito delle proprie competenze istituzionali; attraverso tali strumenti si perseguono finalità di tutela della popolazione e del patrimonio comunale, garantendo quindi un elevato grado di sicurezza nei luoghi di

maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, artistico e culturale, negli edifici pubblici, nel centro storico, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare.

11. L'uso dei dati personali nell'ambito definito dal presente Regolamento, non necessita del consenso degli interessati in quanto viene effettuato per l'esecuzione di un compito di interesse pubblico o comunque connesso all'esercizio di pubblici poteri e allo svolgimento di funzioni istituzionali di cui è investito il Comune.

Art. 5 – Caratteristiche tecniche dell'impianto

1. Il sistema si compone di una rete di comunicazione dati e di telecamere collegate alla sala operativa della Polizia Municipale ubicata presso la sede del comando.
2. Il sistema è a circuito chiuso ed i relativi elaboratori non sono interconnessi con altri sistemi, archivi o banche dati, né accessibili da altre periferiche.
3. In relazione ai principi di pertinenza e di non eccedenza già richiamati all'art. 2 del presente regolamento, il sistema informativo ed 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. 6 – Informativa

1. Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata mediante appositi cartelli conformi ai modelli approvati dall'Autorità garante per la protezione dei dati personali.
2. L'ente, in particolare, si obbliga ad affiggere la richiamata segnaletica, nelle aree in cui sono posizionate le telecamere, su cui è riportata la seguente dicitura: "Area videosorvegliata – la registrazione è effettuata dal Comune di Comune di Canicattini Bagni, con l'indicazione della natura e finalità del controllo.
3. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, andranno installati più cartelli informativi.
4. Sul sito istituzionale del Comune è pubblicata l'informativa contenente le modalità e le finalità per cui gli impianti di videosorveglianza, la modalità di raccolta e conservazione dei dati e le modalità di diritto di accesso dell'interessato secondo quanto previsto dal Regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e al relativo D.lgs.51/2018, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagini, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

Art. 7 - Valutazione di Impatto sulla protezione dei dati

1. In ossequio al disposto di cui all'art. 35, Paragrafo 3, lett. c), RGPD, qualora il trattamento di dati realizzato mediante il sistema di videosorveglianza comunale dia luogo ad una sorveglianza sistematica su larga scala di una zona accessibile al pubblico, l'Ente procederà ad una valutazione di impatto sulla protezione dei dati personali.
2. Parimenti si procederà nei casi in cui, il trattamento di dati realizzato mediante il sistema di

videosorveglianza presenti un rischio comunque elevato per i diritti e le libertà delle persone fisiche.

Art. 8 - Titolare e Responsabili del Trattamento dei dati

1. Il Titolare del trattamento dei dati è il Comune di Canicattini Bagni (nella persona del Sindaco Pro-Tempore), al quale compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza da adottare.
2. Il Responsabile del Comando di Polizia Municipale è designato quale Responsabile del trattamento dei dati personali rilevati attraverso il sistema di videosorveglianza.
3. Il Responsabile ha l'obbligo di attenersi a quanto previsto dalla normativa vigente in tema di trattamento dei dati personali, ivi incluso il profilo della sicurezza, ed alle disposizioni del presente Regolamento.
4. Il Responsabile procede al trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni previste dalla normativa vigente sulla privacy e delle proprie istruzioni.
5. Le competenze proprie del Responsabile del trattamento sono analiticamente disciplinate nel contratto ovvero nell'atto giuridico avente forma scritta, con il quale il Titolare provvede alla sua designazione.
6. Il Responsabile interno del trattamento è autorizzato a ricorrere a Responsabili esterni del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate che assicurino la tutela dei diritti dell'interessato, **in tutti i casi in cui egli, per la gestione/assistenza del sistema di videosorveglianza, faccia ricorso a soggetti esterni ai quali affidare incarichi, servizi, lavori, forniture o consulenze che comportino un trattamento di dati per conto dell'Ente.**
7. In questi casi, il Responsabile interno del trattamento procederà a disciplinare i trattamenti da parte del responsabile esterno mediante contratto ovvero altro atto giuridico che vincoli il Responsabile esterno del trattamento al Titolare del trattamento ai sensi dell'art. 28, RGPD.

Art. 9 – Incaricati del Trattamento

1. Il Responsabile del trattamento dei dati procede ad individuare con proprio atto, nell'ambito del Comando di Polizia Municipale, le persone fisiche incaricate del trattamento dei dati, dell'utilizzazione degli impianti e della visione delle registrazioni.
2. L'individuazione è effettuata per iscritto e con modalità tali da consentire una chiara e puntuale definizione dell'ambito del trattamento consentito a ciascun incaricato.
3. In ogni caso, prima dell'utilizzo degli impianti, gli incaricati dovranno essere istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento e dovranno conformare la propria condotta al pieno rispetto del medesimo.
4. Gli Incaricati procedono al trattamento attenendosi alle istruzioni impartite dal Responsabile il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.
5. In particolare, gli incaricati devono:
   - per l'accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali di accesso personali, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
   - conservare i supporti informatici contenenti dati personali in modo da evitare che detti supporti

siano accessibili a persone non autorizzate al trattamento dei dati medesimi;

- mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali;
- custodire e controllare i dati personali affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
- evitare di creare banche dati nuove senza autorizzazione espressa del Responsabile del trattamento dei dati;
- mantenere assoluto riserbo sui dati personali di cui vengano a conoscenza in occasione dell'esercizio delle proprie mansioni;
- conservare i dati rispettando le misure di sicurezza predisposte dall'Ente;
- fornire al Responsabile del trattamento, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

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

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

1. L'installazione delle telecamere avviene esclusivamente nei luoghi pubblici (strade, piazze, immobili) ubicati nel territorio comunale secondo le indicazioni dall'Amministrazione Comunale.
2. L'attività di videosorveglianza deve raccogliere solo dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando solo immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando (quando non strettamente indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti.
3. Le telecamere di cui al precedente comma 1, consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario.
4. Il titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone fisiche che non siano funzionali alle finalità istituzionali dell'impianto attivato.
5. I segnali video delle unità di ripresa saranno inviati presso l'Unità di ricezione, registrazione e visione ubicata nell'Ufficio di Polizia Municipale. In questa sede le immagini saranno visualizzate su monitor e registrate su supporto magnetico.
6. I dati personali oggetto di trattamento sono:
   - trattati in modo lecito e secondo correttezza;
   - raccolti e registrati per le finalità di cui all'art. 4 del presente Regolamento;
   - raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati.
7. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata alla luce delle richiamate disposizioni normative nel termine massimo di sette giorni, successivi alla rilevazione delle informazioni e delle immagini raccolte oltre il quale il sistema provvede in automatico alla loro cancellazione con modalità da rendere non più utilizzabili i dati cancellati.
8. In ragione di necessità investigative e su richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria il Responsabile potrà disporre la conservazione delle immagini per un periodo di tempo superiore ai

sette giorni previa richiesta al Garante per la protezione dei dati personali che, a seguito di verifica preliminare, potrà rilasciare parere favorevole.

Art. 11 - Sicurezza dei dati

1. I dati personali oggetto di trattamento sono conservati ai sensi e per gli effetti del precedente art. 10.
2. L'accesso alla sala operativa per la gestione degli impianti di videosorveglianza e dei sistemi di lettura targhe è consentito solamente al personale in servizio del Corpo di Polizia Municipale autorizzato dal Comandante.
3. Eventuali accessi di persone diverse da quelli innanzi indicate devono essere autorizzati di volta in volta, per iscritto, dal Comandante del Corpo di Polizia Municipale.
4. I dati raccolti mediante il sistema di videosorveglianza dovranno essere protetti con idonee e preventive misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato al rischio.
5. Dette misure, in particolare, assicurano:
   a) la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   b) il ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico;
   c) la sistematica e periodica verifica e valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Ai sensi dell'art. 32, Paragrafo 2, RGPD, nel valutare l'adeguato livello di sicurezza, l'Amministrazione terrà conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati dall'Ente.
6. A questo fine, sono adottate le seguenti specifiche misure tecniche e organizzative che consentano al Titolare di verificare l'attività espletata da parte di chi accede alle immagini e/o controlla i sistemi di ripresa:
   a) per quanto riguarda il periodo di conservazione delle immagini, così come già indicato al precedente art. 10, dovranno essere predisposte misure tecniche per la cancellazione, in forma automatica, delle registrazioni, al rigoroso scadere del termine previsto;
   b) nel caso di interventi derivanti da esigenze di manutenzione, si renderà necessario adottare specifiche cautele; in particolare, i soggetti incaricati di procedere a dette operazioni potranno accedere alle immagini oggetto di ripresa solo se ciò si renda indispensabile al fine di effettuare le necessarie verifiche tecniche. Dette verifiche avverranno in presenza dei soggetti dotati di credenziali di autenticazione ed abilitanti alla visione delle immagini;
7. Il Titolare ed il Responsabile del trattamento vigilano sulla condotta tenuta da chiunque agisca sotto la loro autorità e abbia accesso ai dati personali; provvedono altresì ad istruire e formare gli incaricati sulle finalità e sulle modalità del trattamento, sul corretto utilizzo delle procedure di accesso ai sistemi, sugli obblighi di custodia dei dati e, più in generale, su tutti gli aspetti aventi incidenza sui diritti dei soggetti interessati.

Art. 12 – Accesso ai dati

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

di cui all'art. 4 del presente Regolamento.

2. L'accesso alle immagini è consentito esclusivamente:
   a) al Titolare, al Responsabile ed agli incaricati del trattamento;
   b) alle Forze di Polizia (sulla base di richiesta scritta formulata dal rispettivo comando di appartenenza e acquisita dall'Ente) nonché per finalità di indagine dell'Autorità Giudiziaria (sulla base di formale richiesta proveniente dal Pubblico Ministero e acquisita dall'Ente);
   c) alla società fornitrice dell'impianto ovvero al soggetto incaricato della manutenzione nei limiti strettamente necessari alle specifiche esigenze di funzionamento e manutenzione dell'impianto medesimo;
   d) all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso alle immagini, previo accoglimento della relativa richiesta, secondo la procedura descritta al successivo art. 13. L'accesso da parte dell'interessato, sarà limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, dovrà pertanto essere utilizzata, da parte del responsabile del trattamento, una schermatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti;
   e) ai soggetti legittimati all'accesso ai sensi e per gli effetti degli artt. 22 e ss. L. 241/90 e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'art. 24, comma 7, L. 241/90, l'accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente.
3. L'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante.
4. Tutti gli accessi alla visione saranno documentati mediante l'annotazione in un apposito "registro degli accessi" (cartaceo od informatico), conservato nei locali del Comando di Polizia Municipale, 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. 13 – Utilizzo di telecamere mobili

1. La Polizia Municipale può utilizzare, dietro disposizione del Comandante per i servizi a maggior rischio operativo, delle telecamere mobili Body Cam (telecamere a bordo uomo) e delle Dash Cam (telecamere a bordo veicoli) in conformità delle indicazioni dettate dal Garante della Privacy con nota 26 luglio 2016, prot. n.49612, con cui sono state impartite le prescrizioni generali di utilizzo dei predetti dispositivi il cui trattamento dei dati è ridotto nell'ambito dell'art. 35 del Codice Privacy e del D.lgs. 51/2018, trattandosi di "dati personali direttamente correlati all'esercizio dei compiti di polizia, di prevenzione dei reati, di tutela all'ordine pubblico e della sicurezza pubblica, nonché di polizia giudiziaria".

Art.14 – Utilizzo di telecamere modulari

1. Su tutto il territorio comunale possono essere temporaneamente posizionate un adeguato numero di telecamere modulari (foto trappole), per il monitoraggio attivo di luoghi determinati, che vengono posizionati secondo necessità di indagini previste dal D.Lgs. 51/2018, provvedendo alla previa collocazione della adeguata cartellonistica, per l'informativa agli utenti frequentatori di dette aree.

Art. 15 - Diritti dell'interessato

1. In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., RGPD, su presentazione di apposita istanza, ha diritto:
   a) di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;
   b) ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;
   c) di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 RGPD, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21, RGPD.
2. Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:
   - il luogo, la data e la fascia oraria della possibile ripresa;
   - l'abbigliamento indossato al momento della possibile ripresa;
   - gli eventuali accessori in uso al momento della possibile ripresa;
   - l'eventuale presenza di accompagnatori al momento della possibile ripresa;
   - l'eventuale attività svolta al momento della possibile ripresa;
   - eventuali ulteriori elementi utili all'identificazione dell'interessato.
3. Il responsabile della protezione dei dati dell'Ente ovvero il responsabile del trattamento accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.
4. Qualora, ai sensi dell'art. 15, paragrafo 3, RGPD, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15, paragrafo 4, RGPD.
5. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
6. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi.
7. L'interessato può altresì farsi assistere da persona di fiducia.
8. In caso di incidente stradale, se interviene personale del Corpo di Polizia Municipale, provvederà alla richiesta direttamente il personale operante.

9. In caso di intervento di altra forza dell'ordine, opportuno seguire la medesima procedura prevista per i fatti di reato.
10. Ai sensi dell'art.391 quater del C.P.P., gli avvocati hanno titolo ad avere copia delle immagini registrate, purché la richiesta venga presentata in qualità di difensore d'ufficio /di fiducia di un indagato in procedimento penale.
11. E' possibile stipulare apposita convenzione con altri Corpi ed Organi di Polizia competenti territorialmente al fine di consentire la visualizzazione diretta delle immagini degli apparati di videosorveglianza, stabilendo le caratteristiche generali del sistema, le implementazioni e modalità di fruizione dei dati, la titolarità e la responsabilità del trattamento e le misure di sicurezza per proteggere i dati ed il sistema.

Art. 16 – Tutela amministrativa e giurisdizionale

1. Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss, RGPD e al Decreto Legislativo 10 agosto 2018, n. 101 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 (regolamento generale sulla protezione dei dati).

Art. 17 – Provvedimenti attuativi

1. Compete alla Giunta Comunale l'assunzione dei provvedimenti attuativi conseguenti al presente Regolamento.

Art. 18 - Pubblicità del Regolamento

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

Art. 19 – Norma di rinvio

1. Per tutto quanto non disciplinato dal presente Regolamento si fa rinvio alle Leggi vigenti, ai provvedimenti attuativi delle medesime, alle decisioni del Garante e ad ogni altra normativa, speciale, generale, nazionale e comunitaria in materia di protezione e trattamento dei dati personali nell'ambito della videosorveglianza.

Art. 20 – Entrata in vigore

1. Il presente Regolamento entrerà in vigore con la dichiarazione di immediata eseguibilità della deliberazione di approvazione.
2. Il presente regolamento abroga ogni disposizione regolamentare precedente che disciplina tale materia.

COMUNE DI CANICATTINI BAGNI

PROVINCIA DI SIRACUSA

INFORMATIVA GESTIONE DELLE VIDEO RIPRESE SICUREZZA URBANA

SETTORE IV POLIZIA MUNICIPALE E PROTEZIONE CIVILE

Informativa ai sensi dell'art. 13 del Regolamento UE n. 679/2016 GDPR e Codice in materia di protezione dei dati personali(cosiddetta Legge Privacy)

Secondo la normativa indicata, il trattamento relativo al presente servizio sarà improntato ai principi di **correttezza, liceità, trasparenza e di tutela della Sua riservatezza e dei Suoi diritti**.

Ai sensi dell'articolo 13 del GDPR 2016/679, pertanto, Le forniamo le seguenti informazioni:

- **Comune di Canicattini Bagni nel ruolo di Titolare**

- **Globalsystem S.p.A (DPO)Data Protection Officer: Vincenzo Mosca**
  email: dpo@globalsystemspa.it

Finalità del trattamento: Trattare i dati del servizio Gestione delle video riprese sicurezza urbana al fine di Gestire le attività di verifica e controllodi riprese video per la salvaguardia della sicurezza urbana

I dati personali che saranno raccolti e trattati riguardano:

1. Immagini, elementi caratteristici della identità fisica;
2. Dati di localizzazione: ubicazione, GPS, GSM, altro;
3. Targa.

Mentre dati personali particolari che saranno raccolti e trattati riguardano:

1. Posizione debitoria
2. Informazioni comportamentali

Gli interessati al trattamento dei dati appartengono alle seguenti categorie:

1. Utenti;
2. Dipendenti;
3. Amministratori;
4. Cittadini.

Il trattamento non necessita di consenso da parte dell'interessato.
Le categorie dei destinatari sono:

1. Persone fisiche;
2. Autorità pubbliche;
3. Aziende;

Non sono previsti trasferimenti verso Paesi Terzi.

Il trattamento non comporta l'attivazione di un processo decisionale automatizzato e i dati raccolti saranno trattati in liceità, in quanto:

1. GDPR - art.6 Comma 1, e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento
2. Provvedimenti Garante Privacy in materia di videosorveglianza; Reg. Comunale; Art 6 DL 11/2009; DL 14/2017; Direttiva polizia 680/2016

Vi informiamo al fine di eseguire il servizio ci avvaliamo dei seguenti responsabili esterni:

- _____
- _____

I dati personali forniti saranno oggetto di:

1. Registrazione;
2. Conservazione;
3. Uso;
4. Limitazione;
5. Cancellazione o distruzione;

Si informa che, tenuto conto delle finalità del trattamento come sopra illustrate, il conferimento dei dati è obbligatorio ed il loro mancato, parziale o inesatto conferimento potrà avere, come conseguenza, l'impossibilità di svolgere l'attività. Il trattamento sarà effettuato sia con strumenti manuali e/o informatici e telematici con logiche di organizzazione ed elaborazione strettamente correlate alle finalità stesse e comunque in modo da garantire la sicurezza, l'integrità e la riservatezza dei dati stessi nel rispetto delle misure organizzative, fisiche e logiche previste dalle disposizioni vigenti. In particolare sono state adottate le seguenti misure di sicurezza: misure specifiche poste in essere per fronteggiare rischi di distruzione, perdita, modifica, accesso, divulgazione non autorizzata, sistemi di autenticazione, sistemi di autorizzazione, sistemi di protezione (antivirus; firewall; antintrusione; altro) adottati per il trattamento.

I dati personali vengono conservati nelle seguenti modalità:

- Verranno eliminati secondo norme di legge e prassi settoriali Il trattamento sarà digitale.

  Lei potrà, in qualsiasi momento, esercitare i diritti:
- Di richiedere maggiori informazioni in relazione ai contenuti della presente informativa e di accesso ai dati personali;

- Di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano (nei casi previsti dalla normativa); di opporsi al trattamento (nei casi previsti dalla normativa);
- Alla portabilità dei dati (nei casi previsti dalla normativa);
- Di revocare il consenso, ove previsto: la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso conferito prima della revoca;
- Di proporre reclamo all'autorità di controllo (Garante Privacy) di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro per l'esercizio dei suoi diritti, di richiedere il risarcimento dei danni conseguenti alla violazione della normativa (art. 82.)

Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento verranno fornite informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

L'esercizio dei suoi diritti potrà avvenire attraverso contatto diretto e/o l'invio di una richiesta presso Comune di Canicattini Bagni Via Venti Settembre nr.42

L'esercizio dei suoi diritti potrà avvenire attraverso contatto diretto e/o l'invio di una richiesta anche mediante email a:

- Data Protection Officer **: Vincenzo Mosca** - email: dpo@globalsystemspaspa.it
- Titolare: pec: **comune.canicattinibagni@pec.it**

La informiamo che potrà ottenere ulteriori informazioni sul trattamento dei dati e sull'esercizio dei suoi diritti nonché sulla disciplina normativa inmateria al seguente link: http://www.garanteprivacy.it.

Spazio dedicato per eventuale consenso o presa visione

IL TITOLARE

Comune di Canicattini Bagni
Sede: Via Venti settembre, 42
CF: 0094260890

Sito: http://www.comunedicanicattinibagni.it

COMUNE DI CANICATTINI BAGNI

PROVINCIA DI SIRACUSA

INFORMATIVA GESTIONE DEI PROCEDIMENTI SANZIONATORI AMMINISTRATIVI A TUTELA DELL'AMBIENTE E SCARICO RIFIUTI IN LUOGHI NON AUTORIZZATI

SETTORE IV
POLIZIA MUNICIPALE E PROTEZIONE CIVILE

Informativa ai sensi dell'art. 13 del Regolamento UE n. 679/2016 GDPR e Codice in materia di protezione dei dati personali (cosiddetta Legge Privacy)

Secondo la normativa indicata, il trattamento relativo al presente servizio sarà improntato ai principi di **correttezza, liceità, trasparenza e di tutela della Sua riservatezza e dei Suoi diritti.** Ai sensi dell'articolo 13 del GDPR 2016/679, pertanto, Le forniamo le seguenti informazioni:

- **Comune di Canicattini Bagni nel ruolo di Titolare**
- **Data Protection Officer DPO: Vincenzo Mosca - email: dpo@globalsystemspa.it**

Finalità del trattamento: Trattare i dati del servizio Gestione dei procedimenti sanzionatori amministrativi a tutela dell'ambiente e scarico rifiuti in luoghi non autorizzati al fine di Gestione dei procedimenti sanzionatori amministrativi a tutela dell'ambiente e scarico rifiuti in luoghi non autorizzati.

I dati personali che saranno raccolti e trattati riguardano:

1. Dati identificativi: cognome e nome, residenza, domicilio, luogo di nascita;
2. Immagini, elementi caratteristici della identità fisica;
3. Situazione patrimoniale;
4. Dati di localizzazione: ubicazione, GPS, GSM, altro;
5. Nome, Cognome, mail, codice fiscale, partita iva, telefono.

Gli interessati al trattamento dei dati appartengono alle seguenti categorie:

1. Contribuenti;
2. Utenti;
3. Partecipanti al procedimento;
4. Amministratori;
5. Cittadini.

Il trattamento non necessita di consenso da parte dell'interessato.Le categorie dei destinatari sono:

1. Persone fisiche;
2. Autorità pubbliche;
3. Aziende.

Non sono previsti trasferimenti verso Paesi Terzi.

Il trattamento non comporta l'attivazione di un processo decisionale automatizzato e i dati raccolti saranno trattati in liceità, in quanto:

1. GDPR - art.6 Comma 1, e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento
2. D.lgs. 152/2006 e s.m.i., D.lgs. 267/2000 e s.m.i., D.lgs. 36/2003, Legge 257/92, Legge 447/1995, D.P.C.M. 14/11/1997, D.P.R. 59/2013, L.R. 44, D.lg. 51/2018

Vi informiamo al fine di eseguire il servizio ci avvalliamo dei seguenti responsabili esterni:

- Ditta affidataria del servizio comunale di raccolti rifiuti

I dati personali forniti saranno oggetto di:

1. Raccolta;
2. Registrazione;
3. Organizzazione;
4. Strutturazione;
5. Conservazione;
6. Adattamento o modifica;
7. Uso;
8. Limitazione;

Comunicati a Autorità amministrative, enti pubblici preposti alla tutela ambientale e altri organi partecipanti al procedimento amministrativo.

Si informa che, tenuto conto delle finalità del trattamento come sopra illustrate, il conferimento dei dati è obbligatorio ed il loro mancato, parziale o inesatto conferimento potrà avere, come conseguenza, l'impossibilità di svolgere l'attività. Il trattamento sarà effettuato sia con strumenti manuali e/o informatici e telematici con logiche di organizzazione ed elaborazione strettamente correlate alle finalità stesse e comunque in modo da garantire la sicurezza, l'integrità e la riservatezza dei dati stessi nel rispetto delle misure organizzative, fisiche e logiche previste dalle disposizioni vigenti. In particolare sono state adottate le seguenti misure di sicurezza: misure specifiche poste in essere per fronteggiare rischi di distruzione, perdita, modifica, accesso, divulgazione non autorizzata, sistemi di autenticazione, sistemi di autorizzazione, sistemi di protezione (antivirus; firewall; antintrusione; altro) adottati per il trattamento.

I dati personali vengono conservati nelle seguenti modalità:

- 7 GIORNI

Il trattamento sarà digitale.

Lei potrà, in qualsiasi momento, esercitare i diritti:

- Di richiedere maggiori informazioni in relazione ai contenuti della presente informativa e di accesso ai dati personali;
- Di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano (nei casi previsti dalla normativa); di opporsi al trattamento (nei casi previsti dalla normativa);
- Alla portabilità dei dati (nei casi previsti dalla normativa);
- Di revocare il consenso, ove previsto: la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso conferito prima della revoca;
- Di proporre reclamo all'autorità di controllo (Garante Privacy) di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro per l'esercizio dei suoi diritti, di richiedere il risarcimento dei danni conseguenti alla violazione della normativa (art. 82.)

Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento verranno fornite informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

L'esercizio dei suoi diritti potrà avvenire attraverso contatto diretto e/o l'invio di una richiesta presso Comune di Canicattini Bagni Via Venti Settembre, 42.

L'esercizio dei suoi diritti potrà avvenire attraverso contatto diretto e/o l'invio di una richiesta anche mediante email a:

- Data Protection Officer DPO: Vincenzo Mosca - email: dpo@globalsystemspa
- Titolare: pec: **comune.canicattinibagni@pec.it**

La informiamo che potrà ottenere ulteriori informazioni sul trattamento dei dati e sull'esercizio dei suoi diritti nonché sulla disciplina normativa inmateria al seguente link: http://www.garanteprivacy.it.

COMUNE DI CANICATTINI BAGNI

PROVINCIA DI SIRACUSA

Spazio dedicato per eventuale consenso o presa visione

IL TITOLARE

Comune di Canicattini Bagni
Sede: Via Venti settembre, 42
CF: 0094260890

Sito: http://www.comunedicanicattinibagni.it

COMUNE DI CANICATTINI BAGNI

Provincia di Siracusa

DATA PROTECTION IMPACT ASSESSMENT

-

VALUTAZIONE D'IMPATTO

UTILIZZO DI IMPIANTI DI VIDEOSORVEGLIANZA IN AMBITO COMUNALE

Canicattini Bagni lì _____/_____/_____

Sommario

1 Informazioni sulla DPIA 3

1.1 Nome della DPIA 4

2 Premessa 4

2.1 Scopo del documento 4

2.2 Visibilità del documento 4

2.3 Definizioni, acronimi e abbreviazioni 4

3 Contesto 5

3.1 Panoramica del trattamento 5

3.1.1 Quale è il trattamento in considerazione? 5

3.1.2 Quali sono le responsabilità connesse al trattamento? 6

3.1.3 Ci sono standard applicabili al trattamento? 6

3.2 Dati, processi e risorse di supporto 7

3.2.1 Quali sono i dati trattati? 7

3.2.2 Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)? 7

3.2.3 Quali sono le risorse di supporto ai dati? 9

4 Principi Fondamentali 9

4.1 Proporzionalità e necessità 9

4.1.1 Gli scopi del trattamento sono specifici, espliciti e legittimi? 9

4.1.2 Quali sono le basi legali che rendono lecito il trattamento? 10

4.1.3 I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)? 10

4.1.4 I dati sono esatti e aggiornati? 10

4.1.5 Qual è il periodo di conservazione dei dati? 10

4.2 Misure a tutela dei diritti degli interessati 11

4.2.1 Come sono informati del trattamento gli interessati? 11

4.2.2 Ove applicabile: come si ottiene il consenso degli interessati? 12

4.2.3 Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità deidati? 12

4.2.4 Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione(diritto all'oblio)? 13

4.2.5 Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione? 13

4.2.6 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza edisciplinati da un contratto? 13

5 Rischi 13

5.1 Misure esistenti o pianificate 13

5.1.1 Anonimizzazione 13

5.1.2 Controllo degli accessi logici e tracciabilità 14

5.1.3 Sicurezza dei documenti cartacei 14

5.1.4 Protezione contro il malware e vulnerabilità 14

5.1.5 Crittografia *14*

5.1.6 Minimizzazione dei dati *14*

5.1.7 Archiviazione e Backup *14*

5.1.8 Controllo degli accessi fisici *15*

5.1.9 Sicurezza dell'hardware e prevenzione delle fonti di rischio *15*

5.1.10 Manutenzione *15*

5.1.11 Sicurezza dei canali informatici *15*

5.1.12 Politica di tutela della privacy *15*

5.1.13 Misure di sicurezza specifiche *16*

5.2 Accesso illegittimo ai dati 16

5.2.1 Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare? *16*

5.2.2 Quali sono le principali minacce che potrebbero concretizzare il rischio? *16*

5.2.3 Quali sono le fonti di rischio? *16*

5.2.4 Quali misure fra quelle individuate contribuiscono a mitigare il rischio? *17*

5.2.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? *17*

5.2.6 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? *17*

5.2.7 Quali sono le risorse di supporto ai dati?

5.3 Modifiche indesiderate dei dati 17

5.3.1 Quali sarebbero i principali impatti sugli interessati se il rischio si dovesseconcretizzare? *17*

5.3.2 Quali sono le principali minacce che potrebbero consentire la concretizzazione delrischio? *17*

5.3.3 Quali sono le fonti di rischio? *17*

5.3.4 Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio? *17*

5.3.5 Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate? *17*

5.3.6 Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate? *17*

5.4 Perdita di dati 18

5.4.1 Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesseconcretizzarsi? *18*

5.4.2 Quali sono le principali minacce che potrebbero consentire la materializzazionedel rischio? *18*

5.4.3 Quali sono le fonti di rischio? *18*

5.4.4 Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio? *18*

5.4.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? *18*

5.4.6 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? *18*

5.5 Allegato N. 1 –INFORMAZIONI TECNICHE INERENTI AL SISTEMADI VIDEOSORVEGLIANZA 19

Informazioni sulla DPIA

Nome della DPIA

IMPIANTO VIDEOSORVEGLIANZA COMUNALE

DATA CREAZIONE	_____/___/_____
DATA AGGIORNAMENTO	
N. REVISIONE	

1. Premessa

1.1Scopo del documento

La DPIA si rende necessaria, a norma dell'art. 35, ogniqualvolta dal trattamento possa conseguire un rischio elevato per i diritti e le libertà delle persone interessate, anche durante un trattamento già in corso di esecuzione, qualora si verifichi un mutamento nelle finalità di quest'ultimo o una modifica dei dati stessi che comporti **una maggiore percentuale di rischio**.

La valutazione di impatto privacy è necessaria nel caso di sistemi integrati – sia pubblici, sia privati – che collegano telecamere tra soggetti diversi, o nel caso di sistemi intelligenti, capaci di analizzare le immagini ed elaborarle, per rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. È il caso, soprattutto della videosorveglianza pubblica, che consente la visione delle immagini a soggetti diversi e che si avvalgono di appositi software per l'analisi delle immagini e per il lancio degli allarmi in caso di riscontrate anomalie.

La valutazione d'impatto sulla protezione dei dati è sempre richiesta, in particolare, in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico (articolo 35, paragrafo 3, lettera c) del Gdpr) e negli altri casi indicati dal Garante con il provvedimento 467 dell'11 ottobre 2018. In quest'ultima deliberazione, l'Autorità Garante per la Privacy ha individuato un elenco delle tipologie di trattamenti, comunque non esaustivo, da sottoporre a valutazione d'impatto.

Il modello della presente DPIA è stato estratto, senza rielaborazioni sostanziali, dallo strumento PIA (valutazione di impatto sulla protezione dei dati) progettato dalla Commission Nationale de l'Informatique et des Libertés (CNIL v. 2.3.0), autorità di controllo francese, esplicitamente validato e suggerito anche dal Garante per la protezione dei dati personali italiano.

1.1 Visibilità del documento

Il documento è principalmente indirizzato alle persone coinvolte nel lavoro di attuazione della normativa in materia di protezione dati.

1.3 Definizioni, acronimi e abbreviazioni

Espressione/Acronimo	*Definizione/Significato*
Servizio	Utilizzo degli impianti di videosorveglianza attivati nel territorio del **Comune di CANICATTINI BAGNI**
Titolare del trattamento	Ovvero anche solo "Titolare" è secondo l'art. 4 del RGPD è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali". Nel contesto di questo documento, il titolare è il **Comune di CANICATTINI BAGNI** , cui competono le decisioni in ordine alle finalità ed alle modalità del

	trattamento dei dati personali
Responsabile del trattamento	Soggetto/Azienda Fornitrice del Servizio, eventualmente nominata Responsabile del trattamento ai sensi dell'art. 28 del Reg. UE 2016/679
Interessato	La persona fisica cui si riferiscono i dati personali oggetto di trattamento. Trattasi di una persona fisica identificata ovvero identificabile in modo diretto o indiretto
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 ad esempio 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 (GDPR, Articolo 4, Comma 2).
Rischio	Nel contesto del presente documento, il prodotto tra la probabilità di ledere i diritti e le libertà delle persone fisiche a cui i dati personali trattati si riferiscono e l'impatto su tali diritti e libertà che si verrebbe a produrre per l'interessato ove l'evento temuto (c.d. "minaccia") si dovesseverificare.
DPIA/PIA	Data Protection Impact Assessment (Valutazione d'Impatto sulla protezione dei dati)
GDPR/Reg. UE 2016/679	General Data Protection Regulation. 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 (regolamento generale sulla protezione dei dati)

2. Contesto

2.1 Panoramica del trattamento

2.1.1 Quale è il trattamento in considerazione?

Il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza (VDS) attivati nel territorio dell'Ente, operato dal Comune, avviene da parte del Sindaco *pro tempore*, e dei soggetti specificatamente autorizzati.

Per le immagini riprese e/o registrate nel **Comune di Canicattini Bagni** , il titolare dei dati è il Comune medesimo. A tal fine il Comune è rappresentato dal Sindaco, a cui compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza. Per le immagini riprese e/o registrate in altri Comuni, eventualmente convenzionati, il titolare dei dati è il Comune convenzionato.

Le finalità di utilizzo degli impianti di videosorveglianza sono conformi alle funzioni istituzionali attribuite al Comune dalla legge 7 marzo 1986, n. 65 sull'ordinamento della Polizia Municipale, dallo statuto e dai regolamenti comunali, dalla direttiva Polizia 2016/680 attuata con decreto lgs. 18 maggio 2018, n. 51 nonché dal decreto-legge n. 14 del 20 febbraio

2017 convertito in legge n. 48 del 13 aprile 2017 "disposizioni urgenti in materia di sicurezza delle città" e successive modificazioni ed integrazioni e dalle altre disposizioni normative applicabili al Comune.

Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato ai fini di:

- **tutela della sicurezza urbana e della sicurezza pubblica** - attività di prevenzione, indagine, accertamento e perseguimento di atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, tutelare l'ordine, il decoro e la quiete pubblica, monitorare le aree oggetto di deturpazione da parte dell'utenza al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" e dei poteri attribuiti al Sindaco in qualità di autorità locale;
- **tutela del patrimonio comunale** - vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;
- **tutela della sicurezza stradale e controllo della circolazione dei veicoli** - monitorare e controllare la viabilità e i flussi di traffico, accertamento delle violazioni delle norme di comportamento del Codice della Strada, controllo dei varchi, accesso al centro storico e alle zone a traffico limitato;
- **tutela ambientale e polizia amministrativa** - controllare aree specifiche del territorio comunale per prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado, di discarica di materiale e di sostanze pericolose o di abbandono di rifiuti, oltre che svolgere controlli volti ad accertare le violazioni delle norme contenute nei regolamenti dell'Ente;
- unicamente in qualità di **polizia giudiziaria**, prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nell'ambito di attività di P.G.

Nel rispetto delle finalità previste, dalle immagini di videosorveglianza potranno essere acquisiti elementi strettamente necessari alla verbalizzazione di violazioni amministrative, nel rispetto del principio di minimizzazione ex art. 5 RGPD e delle vigenti normative e regolamenti.

2.1.2 Quali sono le responsabilità connesse al trattamento?

Le responsabilità connesse al trattamento come sopra identificato, sono ascrivibili alla gestione delle attività di accesso, salvataggio, archiviazione, nonché nelle attività manutentive legate all'utilizzo degli impianti VDS.

Il trattamento effettuato mediante il prodotto tecnologico si configura come potrebbe potenzialmente configurarsi come sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La presente analisi garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di sistemi di videosorveglianza gestiti e impiegati dal Comune nel proprio territorio, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. Garantisce, altresì, i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento, avuto riguardo anche alla libertà di circolazione nei luoghi pubblici o aperti al pubblico.

La presente valutazione di impatto viene svolta in quanto si intende valutare i rischi associati al trattamento, le misure identificate per attenuarli al fine di evitare che il trattamento effettuato mediante l'utilizzo dello strumento tecnologico messo a disposizione possa, potenzialmente, ledere i diritti e le libertàdegli interessati ai quali i dati si riferiscono.

2.1.3 Ci sono standard applicabili al trattamento?

Non pare siano presenti standard applicabili direttamente al trattamento; tuttavia, l'attività di videosorveglianza, è disciplinata da numerosi provvedimenti:

- Provvedimento generale in materia di videosorveglianza in ambito pubblico e privato del 08 aprile 2010 del Garante della protezione dei dati personali (G.U. n. 99 del 29/04/2010);
- Linee guida sulla Videosorveglianza negli enti locali dell'ANCI del 09 novembre 2010;
- Circolare del Ministero dell'Interno inerente i Sistemi di videosorveglianza e relative specifiche tecniche per i Comuni del 02 marzo 2012 e successive indicazioni;
- Regolamento UE Generale sulla Protezione dei Dati 2016/679 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" (anche "RGPD/GDPR");
- Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali" some modificato ed integrato dal D.Lgs 101/2018;
- Allegato 1 al provvedimento n. 467 dell'11 ottobre 2018, pubblicato sulla Gazzetta Ufficiale n. 269 del

- 19 novembre 2018, inerente all'elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto del Garante della protezione dei dati personali;
- Direttiva UE 2016/680 relativa "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio", recepita con il D.lgs. 51/2018;
- riferimento agli articoli 7 del D.lgs. 51/2018 (sul trattamento di categorie particolari di dati personali), 6 c. 7 del D.L. 11/2009 (sule Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori") e 54 del D.lgs. 267/2000 (Testo Unico Enti Locali);
- DPR del 15 gennaio 2018, n. 15, recante "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia";
- Decreto-legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48, recante "Disposizioni urgenti in materia di sicurezza delle città" e successive modificazioni ed integrazioni del D.L. 14.06.19 n. 53 convertito con modifiche con L. 8 agosto 2019 n. 77.
- Linee guida 03/2019 v.2 del 29 gennaio 2020 pubblicate dall'EDPB, inerenti al trattamento di dati personali attraverso dispositivi video;
- Le regole per installare telecamere del 05 dicembre 2020, il vademecum e le FAQ in materia di videosorveglianza del 03 dicembre 2020 del Garante della protezione dei dati personali.

2.2 Dati, processi e risorse di supporto

2.2.1 Quali sono i dati trattati?

Costituisce videosorveglianza qual complesso di strumenti finalizzati alla vigilanza in remoto, che si realizza a distanza mediante dispositivi di ripresa video, captazione di immagini ed eventuale conseguente analisi, collegati a un centro di controllo.

I dati personali sono raccolti attraverso riprese video e captazione di immagini effettuate da sistemi di telecamere installate in luoghi pubblici ed aperti al pubblico e lungo le arterie stradali di accesso al territorio comunale (comunali e/o provinciali) ubicati nel territorio di competenza.

Gli impianti riprendono e registrano immagini che permettono di identificare in modo diretto o indiretto le persone riprese. Inoltre, sono trattati i dati degli autoveicoli (n. targa) e persone fisiche che circolano in prossimità delle telecamere.

2.2.2 Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il ciclo di vita dei dati prevede i seguenti trattamenti:

Acquisizione, Registrazione, Organizzazione, Conservazione, Consultazione, Raffronto, Interconnessione, Limitazione, Pseudonimizzazione.

L'impianto di VDS in esame, consente riprese video e foto, diurne e notturne, in condizioni sufficienti di illuminazione naturale ed artificiale. L'impianto è sempre in funzione ed è configurato per la registrazione continuativa.

Inoltre le telecamere non sono dotate di microfono né di sensori di rilevamento e biometrico.

Per le informazioni inerenti al numero delle telecamere, schede tecniche di dettaglio, luogo di installazione, finalità perseguita, si rimanda alla tabella allegata alla presente D.P.I.A. (all. 1).

Le telecamere consentono riprese video e sono collegate alla sala di controllo del **Comando di Polizia Municipale**.

Le immagini sono visualizzate in tempo reale su due monitor direttamente presso la sala di controllo ubicata presso il comando di polizia municipale, da personale autorizzato. Il sistema è a circuito chiuso, senza possibilità di accesso da remoto.

Il luogo di salvataggio delle immagini, invece, si trova presso il **Comando Polizia Municipale** del **Comune di Canicattini Bagni** . Il salvataggio avviene su server dedicato, il quale è collegato mediante fibra ottica alla sala di videosorveglianza collocata presso il Comando della Polizia Locale.

Il sistema VDS in uso al Comando di Polizia municipale comprende apparecchi quali:

- Telecamere posizionate presso il territorio comunale la cui finalità è la prevenzione di atti criminosi quali attività di prevenzione, indagine, accertamento e perseguimento di atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, tutelare l'ordine, il decoro e la quiete pubblica, monitorare le aree oggetto di deturpazione da parte dell'utenza al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" e dei poteri attribuiti al Sindaco in qualità di autorità locale;
- Foto trappole e sistemi mobili di videosorveglianza da posizionare in località difficilmente accessibili o sorvegliabili, al solo titolo esemplificativo zone di campagna, strade interpoderali o aree urbane oggetto di degrado. La finalità dell'utilizzo di tali sistemi di controllo è quella di monitorare le aree oggetto di deturpazione da parte dell'utenza laddove non è possibile farlo diversamente, ai fini sia dell'accertamento delle eventuali violazioni amministrative, sia ai fini della deterrenza alla prosecuzione di azioni di degrado da parte della cittadinanza e dell'utenza di passaggio;
- Apparecchi per l'accertamento delle violazioni delle norme di comportamento del Codice della Strada, che consentono la determinazione dell'illecito in tempo successivo, poiché il veicolo oggetto del rilievo è a distanza dal posto di accertamento o comunque nell'impossibilità di essere fermato in tempo utile o nei modi regolamentari, siano esse in postazione fisse o mobili, in presenza o meno dell'operatore. I sistemi elettronici di rilevamento delle infrazioni inerenti violazioni del codice della strada vanno obbligatoriamente segnalate da cartello/informativa anche in base alla disciplina di settore. L'utilizzo di tali sistemi è lecito se sono raccolti solo dati pertinenti e non eccedenti per il perseguimento delle finalità istituzionali del titolare, delimitando a tal fine la dislocazione e l'angolo visuale delle riprese. La ripresa del veicolo non deve comprendere (o deve mascherare), per quanto possibile, la parte del video o della fotografia riguardante soggetti non coinvolti nell'accertamento amministrativo (es. eventuali pedoni o altri utenti della strada). Le fotografie o i video che attestano l'infrazione non devono essere inviati al domicilio dell'intestatario del veicolo, ma l'interessato, ossia la persona eventualmente ritratta nelle immagini, può richiederne copia oppure esercitare il diritto di accesso ai propri dati (fermo restando che dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo);

Per quanto riguarda gli apparati di videosorveglianza modulare riposizionabili, questi vengono installati secondo necessità, nei luoghi teatro di illeciti penali; possono essere utilizzati per accertare illeciti amministrativi, solo qualora non siano altrimenti accertabili con le ordinarie metodologie di indagine e non si possa fare ricorso a strumenti e sistemi di controllo alternativi e nel rispetto del principio di minimizzazione.

Le immagini sono visualizzate in tempo reale su monitor, direttamente presso il Comando della Polizia Municipale, da personale autorizzato e vengono salvate su un server comunale presente presso il Comando di Polizia Municipale.

Il sistema è a circuito chiuso, senza possibilità di accesso da remoto.

Possono essere autorizzati all'accesso alla sala di controllo solo incaricati di servizi rientranti nei compiti istituzionali dell'Ente o Organismo di appartenenza e per scopi connessi alle finalità individuate nell'apposito regolamento comunale, nonché il personale addetto alla manutenzione degli impianti ed alla pulizia dei locali, preventivamente individuato dal titolare o dal designato al trattamento.

L'accesso alla sala, da parte di soggetti diversi da quelli indicati sopra è subordinato al rilascio, da parte del Titolare, di un'autorizzazione scritta, motivata e corredata da specifiche indicazioni in ordine ai tempi ed alle modalità dell'accesso. L'accesso avviene in presenza di incaricati del Comune.

Gli autorizzati al trattamento e i preposti sono gli unici dotati di proprie credenziali di autenticazione di accesso al sistema. Il sistema dovrà essere fornito di "log" di accesso.

Infatti, l'accesso ai sistemi che gestiscono i dati oggetto dello specifico trattamento, può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide e strettamente personali, rilasciate su disposizione del designato del trattamento come individuato.

L'accesso ai sistemi di registrazione prevede l'adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei designati da parte del titolare, comunque non inferiore a sei mesi.

Per quanto attiene invece il collegamento tra le due sale (ovvero tra i server e il client) questo è protetto da misure di sicurezza tecnica specifiche quale la crittografia e il firewall.

Il personale autorizzato della sala controllo del Comando di Polizia Municipale potrà visionarle esclusivamente per il perseguimento dei fini istituzionali:

a) sulla base di denunce di atti criminosi da parte dei cittadini, per il successivo inoltro delle eventuali fonti di prova all'autorità giudiziaria;
b) sulla base di segnalazioni relative ad atti criminosi accertate direttamente dagli organi di polizia in servizio sul territorio cittadino;
c) sulla base di atti criminosi che vengono rilevati direttamente dagli operatori di polizia nel visionare le immagini trasmesse in diretta dalle telecamere, nell'esercizio delle proprie funzioni.
d) sulla base di richieste specifiche per indagini da parte dell'autorità giudiziaria;
e) sulla base di ogni altra richiesta di specifici organi/autorità che siano espressamente autorizzati, secondo specifiche norme di legge.

Le immagini rilevanti ogni sorta di infrazione o reato vengono scaricate in locale attraverso il dispositivo di memoria di massa e messe a disposizione in caso di necessità agli operatori di giustizia.

Qualora la presa in carico delle immagini e delle videoriprese venga effettuata tramite riversamento dai supporti di memoria presenti negli strumenti di acquisizione, i file contenenti dati devono essere rimossi dai supporti una volta acquisiti i dati. In caso di dismissione di supporti di memorizzazione, questi devono essere resi inutilizzabili tramite danneggiamento fisico irreparabile, in modo che non sia non consentito in alcun modo il recupero dei dati trattati.

Le immagini videoregistrate sono conservate:

- per il periodo ordinariamente non superiore a 7 giorni successivi alla rilevazione, che possono essere estesi fino a 90 giorni tenuto conto delle esigenze specifiche e documentate di indagine e di prevenzione dei reati, con particolare su esplicita richiesta dell'Autorità. L'estensione dei tempi di conservazione, fino a 90 giorni, devono essere sostenute da specifiche ed evidenti esigenze investigative e di polizia giudiziaria nonché specifiche richieste da parte dell'Autorità prefettizia e giudiziaria, tenuto conto di eventuali ulteriori necessità di conservazione in caso di ricorsi;
- per le telecamere a tutela del solo patrimonio comunale per un periodo non superiore a 72 ore successive alla rilevazione, fatte salve speciali e diverse esigenze debitamente documentate.

Al termine del periodo stabilito il sistema di videoregistrazione provvede in automatico alla loro cancellazione ¬ove tecnicamente possibile - mediante sovra-registrazione, con modalità tali da rendere nonpiù utilizzabili i dati cancellati.

In caso di esercizio dei diritti da parte dell'interessato, svolte secondo le procedure come dettagliate nei paragrafi a seguire, in ogni caso di accoglimento delle richieste, l'addetto incaricato dal Titolare del trattamento dei dati deve lasciare traccia delle operazioni eseguite al fine di acquisire i filmati e riversarli su supporto digitale, in modo da garantire la genuinità dei dati stessi.

2.2.3 Quali sono le risorse di supporto ai dati?

Persone:

2.2.3.1 Sindaco;
2.2.3.2 Personale interno formato ed autorizzato (Comandante, Agenti di Polizia Municipale).

Hardware - Software:

2.2.3.3 Infrastruttura HW e SW .

3. Principi Fondamentali

3.1 Proporzionalità e necessità

3.1.1 Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento dei dati personali, acquisiti mediante l'impianto di VDS gestito dall'Ente e collegato alla centrale di controllo ubicata presso gli Uffici dell'Ente, si svolge nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

L'utilizzo dell'impianto comporta esclusivamente il trattamento di dati personali rilevati mediante le riprese video e foto che, in relazione ai luoghi di installazione delle telecamere, interessano i soggetti ed i mezzi di trasporto che transitano nell'area oggetto di sorveglianza.

3.1.2 Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica del trattamento è data dalla necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri ai sensi dell'art. 6, par. 1, lett. e) del Regolamento UE, nonché dalla necessità di eseguire un compito di un'autorità competente per le finalità di prevenzione, accertamento e prevenzione dei reati, salvaguardia e prevenzione contro minacce alla sicurezza pubblica (art. 5 D. Lgs. 51/2018).

In ossequio al disposto di cui sopra, il trattamento dati è effettuato dal Comune esclusivamente per lo svolgimento delle funzioni istituzionali.

3.1.3 I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

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

Nel rispetto del **principio di non eccedenza** i sistemi sono configurati in modo da raccogliere esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo di visuale delle riprese ed evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari rilevanti. La localizzazione delle telecamere e le modalità di ripresa saranno quindi stabilite in modo conseguente.

Nel rispetto del **principio di necessità**, in ambito pubblico è bene precisare che la rilevazione dei dati non potrà essere estesa ad ambiti, aree o attività che non presentino rischi concreti o non caratterizzate da esigenze di dissuasione e deterrenza. Allo stesso modo, laddove la finalità venga individuata nella protezione del bene o dei beni a fronte di atti di vandalismo, il posizionamento di sistemi di videosorveglianza potrà essere considerato lecito solo laddove sia stata valutata l'inefficacia di misure alternative e meno impattanti, quali ad esempio controlli da parte del personale di sicurezza, sistemi di allarme, misure di sicurezza apposte agli ingressi o autorizzazioni all'accesso fisico degli edifici.

In attuazione del **principio di proporzionalità**, nella commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un'effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo qualora altre misure siano state preventivamente ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti (es. controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi). In ogni caso l'Ente garantisce che il trattamento deve essere effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da controllare e/o proteggere.

3.1.4 I dati sono esatti e aggiornati?

I dati vengono aggiornati periodicamente, almeno su base annuale e incrociati con le banche dati nazionali.

3.1.5 Qual è il periodo di conservazione dei dati?

I dati personali oggetto di trattamento sono conservati presso la sala di controllo, alla quale può accedere il solo personale autorizzato secondo istruzioni che devono essere impartite in forma scritta dal designato del trattamento dei dati.

I dati personali registrati mediante l'utilizzo dell'impianto di VDS di cui alla presente analisi, sono conservati per un periodo di tempo non superiore a **sette giorni** dalla data della rilevazione. Decorso tale periodo, i dati registrati sono sovrascritti automaticamente oppure tramite accesso manuale con password da parte dei soggetti autorizzati. Più precisamente, le immagini videoregistrate sono conservate:

3.1.5.1 per il periodo ordinariamente non superiore a 7 giorni successivi alla rilevazione, che possono essere estesi fino a 90 giorni tenuto conto delle esigenze specifiche e documentate di indagine e di prevenzione dei reati. L'estensione dei tempi di conservazione, fino a 90 giorni, devono essere sostenute da specifiche ed evidenti esigenze investigative e di polizia giudiziaria nonché specifiche richieste da parte dell'Autorità prefettizia e giudiziaria, tenuto conto di eventuali ulteriori necessità di conservazione in caso di ricorsi;

3.1.5.2 per le telecamere a tutela del solo patrimonio comunale (o per altre telecamere non collegate alla centrale operativa del Corpo di Polizia Municipale) per un periodo non superiore a 72 ore successive alla rilevazione, fatte salve speciali e diverse esigenze debitamente documentate.

I dati personali registrati mediante l'utilizzo dell'impianto di VDS di cui alla presente analisi, sono conservati per un periodo di tempo non superiore a **sette giorni** dalla data della rilevazione. Decorso tale periodo, i dati registrati sono sovrascritti automaticamente oppure tramite accesso manuale con password da parte dei soggetti autorizzati, il periodo di conservazione può essere esteso fino a 90 giorni tenuto conto delle esigenze specifiche e documentate di indagine e di prevenzione dei reati. L'estensione dei tempi di conservazione, fino a 90 giorni, deve essere sostenuta da specifiche ed evidenti esigenze investigative e di polizia giudiziaria nonché specifiche richieste da parte dell'Autorità prefettizia e giudiziaria, tenuto conto di eventuali ulteriori necessità di conservazione in caso di ricorsi.

Gli strumenti e i supporti elettronici utilizzati sono dotati del sistema di protezione informatica quale log-in e password per accesso alle apparecchiature.

3.2 Misure a tutela dei diritti degli interessati

3.2.1 Come sono informati del trattamento gli interessati?

Gli interessati sono informati mediante:

- pubblicazione del regolamento elaborato e adottato dall'Ente, comprensivo dei dettagli e di altra documentazione relativa alle zone video-sorvegliate e foto-sorvegliate, sul sito web istituzionale dell'Ente;
- installazione di apposita segnaletica permanente, contenente l'informativa breve, nelle aree in cui sono concretamente posizionate le telecamere;
- informativa completa, contenente gli elementi di cui agli articoli 12-13-14 del GDPR, disponibile agevolmente e senza oneri per gli interessati, sul sito web e nei locali dell'Ente, in modo da essere resa facilmente accessibile anche con strumenti informatici o telematici.

La segnaletica viene collocata prima del raggio di azione di ogni telecamera, o nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa è predisposta in modo da avere un posizionamento chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di VDS sia eventualmente attivo in orario notturno. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, sono installati più cartelli informativi.

L'Ente, in qualità di Titolare del trattamento, provvede ad informare la comunità cittadina dell'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di VDS, dell'eventuale incremento dimensionale dell'impianto stesso e successiva cessazione per qualsiasi causa del trattamento medesimo e si obbliga ad affiggere la richiamata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere.

L'informativa di cui sopra non è dovuta nel caso di utilizzo di telecamere a scopo investigativo a tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati.

3.2.2 Ove applicabile: come si ottiene il consenso degli interessati?

Considerato che il Titolare del trattamento è una pubblica amministrazione che eroga servizi pubblici legalmente attribuiti, non è tenuto all'acquisizione del consenso al trattamento dei dati; nel caso in cui questo sia dovuto, viene acquisito per iscritto.

3.2.3 Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità deidati?

Gli interessati potranno esercitare i propri diritti rivolgendosi al Titolare del trattamento secondo le modalità da lui stesso individuate e comunicate agli interessati attraverso l'informativa predisposta.

Il Titolare, qualora lo ritenga necessario, richiederà l'eventuale intervento del Responsabile del trattamento; lo stesso avverrà come indicato nel contratto di nomina, ad es. fornendo supporto nell'estrazione dei dati in formato strutturato.

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

- di ottenere dal Titolare del trattamento, la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;
- ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;
- di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 del GDPR, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21 del GDPR.

L'istanza per l'esercizio dei diritti, da parte dell'interessato, è presentata al DPO dell'Ente, ai sensi dell'art. 38 par.4 del GDPR ovvero al Responsabile del trattamento eventualmente individuato e può essere presentata mezzo posta certificata PEC: **comune.canicattinibagni@pec.it**

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

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

Il Responsabile individuato, appositamente autorizzato al trattamento dei dati personali, avrà cura di accertare l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; in caso di accertamento positivo, fisserà il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.

Qualora l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, ai sensi dell'art. 15 par. 3 del GDPR, si procederà al rilascio dei file contenenti le immagini, in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa (art. 15 par. 4 del GDPR).

I diritti come sopra esplicitati, riferiti ai dati personali concernenti persone decedute, possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato per ragioni familiari meritevoli di protezione.

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

Qualora non sia possibile identificare l'interessato (o in caso di richieste eccessive o manifestamente infondate) il designato – previa adeguata motivazione ed entro i termini di 7 giorni dalla richiesta – informerà l'interessato dell'impossibilità di dare seguito alla richiesta.

In caso di esito negativo all'istanza dell'interessato, quest'ultimo potrà rivolgersi al Garante della protezione dei dati personali per il reclamo, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Al fine di:

- non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;
- non compromettere l'attività di prevenzione, indagine, accertamento e perseguimento di reati o l'esecuzione di sanzioni penali;
- proteggere la sicurezza pubblica;
- proteggere la sicurezza nazionale;

potranno essere adottate misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessai della persona fisica interessata.

3.2.4 Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo.

Per esercitare il diritto alla cancellazione, se possibile in ragione dell'obbligo dell'Ente di conservazione delle informazioni, gli interessati possono contattare direttamente il Titolare del trattamento ovvero il DPO ovvero il responsabile esterno eventualmente individuato, recandosi direttamente presso l'Ente, mediante invio di raccomandata ovvero di posta certificata, ai canali di contatto indicati dal Titolare all'interno dell'informativa.

3.2.5 Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Per esercitare il diritto di limitazione o opposizione, se possibile in ragione degli obblighi in capo all'Ente, gli interessati possono contattare direttamente il Titolare del trattamento ovvero il DPO ovvero il responsabile esterno eventualmente individuato, recandosi direttamente presso l'Ente, mediante invio di raccomandata ovvero di posta certificata, ai canali di contatto indicati dal Titolare all'interno dell'informativa.

3.2.6 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Il rapporto di responsabilità tra il Titolare ed il responsabile esterno eventualmente individuato è definito e disciplinato da un contratto di appalto dei relativi servizi ovvero mediante specifica comunicazione.

Inoltre, gli obblighi derivanti dal trattamento incidentale dei dati trattati mediante l'utilizzo dell'impianto, sono disciplinati in apposito allegato per la nomina conforme alle disposizioni previste dall'art. 28 Reg. UE 2016/679.

3.2.7 In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati non vengono trasferiti al di fuori dello spazio SEE.

4. Rischi

4.1 Misure esistenti o pianificate

4.1.1 Anonimizzazione

I dati particolari, i c.d. sensibili, eventualmente rilevati vengono trattati in maniera riservata unicamente dal personale strettamente necessario e a questo autorizzato. I dati oggetto di trattamento vengono resi sempre anonimi.

4.1.2 Controllo degli accessi logici e tracciabilità

- Individuazione di postazione informatica dedicata dotata di username e password personale di accesso per ogni operatore (unico e tracciabile);
- il software prevede la registrazione e conseguente tracciabilità degli accessi logici e delle operazioni effettuate dagli autorizzati al trattamento dei dati.
- Assegnazione, ad uso esclusivo, di una o più credenziali di autenticazione agli operatori;
- Assegnazione di parole chiave che rispondono ai requisiti di sicurezza e che sono modificateciclicamente;
- Aggiornamento periodico delle credenziali di autenticazione;
- Attivazione di uno screensaver automatico, dopo pochi minuti di non utilizzo, con inserimento password per la prosecuzione del lavoro;
- Disattivazione delle credenziali di autenticazione nel caso di inutilizzo perdurato ovvero in caso di perdita di qualità dell'incaricato.

4.1.3 Sicurezza dei documenti cartacei

I documenti cartacei vengono conservati dai dipendenti dell'ufficio in conformità a quanto previsto dalle procedure aziendali di riferimento, in maniera tale da garantire la riservatezza e la non visibilità a terzi nonautorizzati.

4.1.4 Protezione contro il malware e vulnerabilità

- Installazione e aggiornamento periodico di sistemi antivirus e antimalware;
- Aggiornamento costante dei software utilizzati;
- Utilizzo di un sistema Firewall sugli elaboratori ed aggiornamento periodico;
- Aggiornamento periodico dei programmi antivirus;
- Utilizzo di filtro anti-spam ed aggiornamento periodico;
- Protezione della posta elettronica con disposizione di verifica della provenienza delle e-mail e di non esecuzione dei file allegati ai messaggi senza preventiva scansione antivirus;
- Disposizione di utilizzo della casella di posta elettronica dell'ufficio come strumento di lavoro e dunque esclusivamente per esigenze lavorative;
- Controllo degli accessi a siti internet non sicuri;
- Divieto di scaricare software e di installare programmi da siti poco attendibili o non ufficiali;
- Disposizione di tenere sempre attiva l'opzione del browser "richiedi conferma" per l'installazione e il download di oggetti sulla propria macchina;
- Reinstallazione dei programmi danneggiati o distrutti.

4.1.5 Crittografia

La crittografia avanzata è applicata alle informazioni che transito dal server, presente presso la sala CED, alla sala operativa, presente presso gli uffici della Polizia Locale.

4.1.6 Minimizzazione dei dati

Vengono raccolti e conservati unicamente i dati necessari e non sono richiesti dati eccedenti le finalità individuate.

4.1.7 Archiviazione e Backup

L'archiviazione dei dati personali trattati avviene in conformità alle procedure comunali di riferimento, garantendo la riservatezza e l'integrità dei dati personali trattati. Ogni dipendente, autorizzato al trattamento, è tenuto ad archiviare i documenti cartacei negli appositi raccoglitori e a conservare/salvare i documenti digitali sulle apposite apparecchiature in uso, protette da password di accesso.

Inoltre, le immagini rilevate dal sistema di VDS non sono oggetto di back-up. Il sistema di back-up è presente soltanto sui client delle immagini esportate.

4.1.8 Controllo degli accessi fisici

- Gli accessi fisici agli uffici sono limitati e controllati;
- Chiavi dei locali custodite dal solo personale della Polizia Municipale;
- Lucchetto porta esterna;
- Server custodito in armadio dedicato dotato di serratura.

4.1.9 Sicurezza dell'hardware e prevenzione delle fonti di rischio

- Manutenzione programmata degli strumenti;
- Distruzione di tutti i supporti removibili non utilizzati;
- Estintori e loro revisione periodica;
- Porte tagliafuoco;
- Accordo di assistenza continuativa con ditta di sicurezza;
- Manutenzione costante impianti e apparecchiature elettriche ed elettroniche;
- Monitoraggio e impegno della direzione nel controllo delle regole in materia di salute e sicurezza sui luoghi di lavoro.

4.1.10 Manutenzione

- Manutenzione programmata degli strumenti
- Manutenzione costante impianti e apparecchiature elettriche ed elettroniche;
- Controllo sull'operato degli addetti alla manutenzione.

4.1.11 Sicurezza dei canali informatici

- Sicurezza dell'infrastruttura di sistema;
- La crittografia avanzata è applicata alle informazioni che transito dal server, presente presso la sala CED, alla sala operativa, presente presso gli uffici della Polizia Municipale;
- Controlli periodici sul sistema di protezione nella trasmissione dei dati;
- Installazione ed aggiornamento periodico del Firewall.

4.1.12 Politica di tutela della privacy

Relativamente alla propria organizzazione, l'Ente, partendo dall'analisi del proprio organigramma, ha ritenuto necessario predisporre una struttura interna per la gestione della privacy, con identificazione dei ruoli, distribuzione dei compiti e delle responsabilità. All'interno della struttura, il trattamento viene effettuato solo da soggetti che hanno ricevuto un formale incarico mediante designazione per iscritto di ogni singolo incaricato (o per categorie omogenee di trattamento). Le responsabilità sono dettagliate per iscritto nella lettera di nomina. Inoltre, sono adottate misure quali:

- Formazione sugli aspetti principali della Regolamento Europeo al momento dell'ingresso in servizio;
- Formazione periodica e in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti per il trattamento dei dati e la loro protezione;
- Istruzioni agli incaricati, finalizzate al controllo e alla custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento senza l'ausilio di strumenti elettronici;
- Istruzioni in merito alla protezione dello strumento elettronico in caso di assenza temporanea durate le sessioni di lavoro;
- Istruzioni in merito alla segretezza e alla custodia delle credenziali di autenticazione;
- Istruzioni in merito all'accesso agli archivi digitali;
- Istruzioni organizzative e tecniche per la custodia dei supporti removibili su cui sono memorizzati i dati;
- Individuazione del profilo di autorizzazione anteriormente all'inizio del trattamento;
- Aggiornamento periodico o al verificarsi di eventuali modifiche della lista degli incaricati e dei profili di autorizzazione;
- Procedure di verifica sull'operato degli incaricati;
- Definizione di responsabilità e sanzioni disciplinari;
- Definizione delle procedure di convalida delle operazioni a rischio nell'ambito dell'incaricoassegnato;

- Controllo degli accessi ai dati e programmi;
- Controllo sull'operato degli addetti alla manutenzione;
- Definizione di procedure per le copie di sicurezza, la loro custodia e il ripristino dei dati;
- Monitoraggio continuo delle sessioni di lavoro;
- Formazione professionale.

4.1.13 Misure di sicurezza specifiche

Ai sensi di quanto previsto dall'art. 24 del GDPR, i dati personali acquisiti mediante l'impiego dell'impianto VDS sono protetti da misure di sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato e trattamento non consentito o non conforme alle finalità di qui al par. 2.1.1. del presente documento.

Ai sensi dell'art. 29 co.2 della Direttiva UE 2016/680 il Titolare del trattamento, previa valutazione dei rischi mette in atto misure volte a:

- vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento ("controllo dell'accesso alle attrezzature");
- impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate ("controllo dei supporti di dati");
- impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione ("controllo della conservazione");
- impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati ("controllo dell'Utente") e garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali ci si riferisce la loro autorizzazione d'accesso ("controllo dell'accesso ai dati");
- garantire la possibilità di verificare e accertare gli organismi ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione dei dati ("controllo della trasmissione");
- garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il moment della loro introduzione e la persona che l'ha effettuata ("controllo dell'introduzione");
- impedire che i dati personali possano essere letti, copiati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati ("controllo del trasporto");
- garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati ("recupero");
- garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati ("affidabilità") e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema ("integrità").

4.2 Accesso illegittimo ai dati

4.2.1 Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Diffusione non autorizzata, intercettazione di informazioni in rete, pregiudizio alla reputazione.

4.2.2 Quali sono le principali minacce che potrebbero concretizzare il rischio?

Abuso di privilegi, accesso non autorizzato ai sistemi aziendali per operazioni non consentite/non autorizzate, furto nei locali aziendali, vulnerabilità degli assets, azione di virus informatici o di programmi suscettibili di recare danno, distruzione totale o parziale e/o diffusione non autorizzata e/o inibizione dell'accesso ai dati, spamming o tecniche di sabotaggio.

4.2.3 Quali sono le fonti di rischio?

Fonti di rischio interne ed esterne anche non umane come attacchi informatici, Virus e Malware.

4.2.4 Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Anonimizzazione, Controllo degli accessi logici e tracciabilità; Sicurezza dei documenti cartacei; Protezione contro i malware e vulnerabilità; Crittografia; Minimizzazione dei dati; Controllo degli accessi fisici;

Manutenzione; Sicurezza dei canali informatici, Politica di tutela della privacy; Misure di sicurezzaspecifiche.

4.2.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

In considerazione dei dati oggetto di trattamento, il rischio individuato è da considerarsi Basso.

4.2.6 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata.

Le misure individuate, pianificate ed adottate contribuiscono a mitigare i rischi individuati.

4.3 Modifiche indesiderate dei dati

4.3.1 Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Alterazione dei dati, negazione dell'accesso a servizi, pregiudizio alla reputazione.

4.3.2 Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Accesso ai dati da parte di soggetti non autorizzati e/o accesso ai dati per trattamenti non consentiti, sottrazione di credenziali di autenticazione, accesso ai dati da parte di soggetti in orari non consentiti, errore umano, carenza di consapevolezza, disattenzione, incuria o indisponibilità, comportamenti contrari ai principi di sicurezza e protezione dei dati, comportamenti sleali o fraudolenti, operazioni accidentali non consentite e/o contrarie ai principi di sicurezza e protezione dei dati.

4.3.3 Quali sono le fonti di rischio?

Utenti e esterni all'organizzazione, attacchi informatici.

4.3.4 Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici e tracciabilità; Protezione contro i malware e vulnerabilità; Crittografia; Minimizzazione dei dati; Archiviazione e back-up; Controllo degli accessi fisici; Sicurezza dei canali informatici, Politica di tutela della privacy; Misure di sicurezza specifiche.

4.3.5 Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

In considerazione dei dati oggetto di trattamento, il rischio individuato è da considerarsi Basso.

4.3.6 Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Limitata.

Le misure individuate, pianificate ed adottate contribuiscono a mitigare i rischi individuati.

4.4 Perdita di dati

4.4.1 Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesseconcretizzarsi?

Indisponibilità dei dati, danno reputazionale.

4.4.2 Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Errori umani nella gestione della sicurezza fisica, eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o dovuti ad incuria, malfunzionamento, guasti, eventi naturali, alterazioni delle trasmissioni, indisponibilità o degrado degli strumenti, guasto ai sistemi complementari, sottrazione di strumenti contenenti dati, comportamenti sleali o fraudolenti, errore materiale, sottrazione di credenziali di autenticazione, azione di virus informatici o di programmi suscettibili di recare danno.

4.4.3 Quali sono le fonti di rischio?

Utenti e esterni all'organizzazione, attacchi informatici, eventi calamitosi, malfunzionamenti.

4.4.4 Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici e tracciabilità; Protezione contro i malware e vulnerabilità; Crittografia; Minimizzazione dei dati; Archiviazione e back-up; Controllo degli accessi fisici; Sicurezza dell'hardware e prevenzione delle fonti di rischio; Sicurezza dei canali informatici, Politica di tutela della privacy; Misure di sicurezza specifiche.

4.4.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

In considerazione dei dati oggetto di trattamento, il rischio individuato è da considerarsi Basso

4.4.6 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata.

Le misure individuate, pianificate ed adottate contribuiscono a mitigare i rischi individuati.

4.5 Allegato N. 1–INFORMAZIONI TECNICHE INERENTI AL SISTEMADI VIDEOSORVEGLIANZA

ID	Luogo di installazione	Finalità di utilizzo	*Nr. Telecamere*
1	**Palazzo Municipale**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n. 1 Telecamera lettura Targhe* *n. 3 Telecamere di contesto*
2	**Comando Polizia Municipale**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n. 1 Telecamere di contesto*
3	**Chiesa Madre**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n. 1 Telecamera lettura Targhe* *n. 1 Telecamere di contesto*
4	**Piazza XX Settembre isola pedonale**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n.1 Telecamere di contesto tipo Dome*
5	**Palazzo Cianci**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n. 1 Telecamera lettura Targhe* *n. 2 Telecamere di contesto*
6	**Via A. Uccello Sede Teatro Comunale**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n. 1 Telecamera lettura Targhe* *n. 1 Telecamere di contesto*
7	**Via Roma " Vera Cruci"**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa;	*n. 1 Telecamera lettura Targhe* *n. 1 Telecamere di contesto*

		- Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	
8	**Via Don Sturzo incrocio via Solferino**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n. 1 Telecamera lettura Targhe* *n. 1 Telecamere di contesto*
9	**Via Giovanni Falcone**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n. 1 Telecamera lettura Targhe* *n. 1 Telecamere di contesto*
10	**Via Canale "Piazzetta Cultrera"**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n. 1 Telecamera lettura Targhe* *n. 2 Telecamere di contesto*
11	**Piazza Borsellino**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n. 1 Telecamera tipo dome* *n. 1 Telecamere di contesto*
12	**Via Vitt. Emanuele "Ingresso Paese"**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n. 1 Telecamera lettura Targhe* *n. 1 Telecamere di contesto*
13	**Ingresso comune Via P.Iolanda**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n. 1 Telecamere di contesto*
14	**Pompa di rilancio c.da Palombara**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n. 2 Telecamere di contesto*
15	**Campo Sportivo**	Le finalità perseguite sono:	*n. 4 Telecamere di contesto*

		- Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	
16	**Via Cavour "Semarofo"**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n. 1 Telecamera lettura Targhe* *n. 1 Telecamere di contesto*
17	**Via Carducci "Piazzetta Dante Alighieri"**	Le finalità perseguite sono: - Tutela della sicurezza urbana e della sicurezza pubblica; - Tutela del patrimonio comunale; - Tutela ambientale e polizia amministrativa; - Tutela della sicurezza stradale e controllo della circolazione dei veicoli.	*n. 1 Telecamera lettura Targhe* *n. 1 Telecamere di contesto*