



Comune di Noragugume

Provincia di Nuoro

Piazza IV Novembre 1, 08010 Noragugume NU

☎ 0785 44743

Email: info@comune.noragugume.nu.it

PEC: protocollo@pec.comune.noragugume.nu.it

Ufficio Tecnico

REGOLAMENTO

PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA NEL TERRITORIO COMUNALE DI NORAGUGUME

Approvato con delibera del Consiglio Comunale del 13/10/2022 n.20

Indice

CAPO I	4
PRINCIPI GENERALI	4
1.1 Oggetto.....	4
1.2 Ambito di applicazione e principi generali.....	4
1.3 Definizioni	5
1.4 Normativa di riferimento	6
CAPO II.....	7
FINALITÀ DEL TRATTAMENTO	7
2.1 Finalità del trattamento	7
2.1.1 Monitoraggio del traffico.....	8
2.1.2 Sicurezza urbana	8
2.1.3 Abbandono di rifiuti e vigilanza ambientale.....	9
2.1.4 Rilevazione di infrazioni al codice della strada e di accesso alle ZTL	Errore. Il segnalibro non è definito.
2.1.5 Body cam e dash cam	9
2.1.6 Telecamere modulari (fototrappole)	10
2.1.7 Istituti scolastici	10
CAPO III.....	11
RUOLI E COMPITI DEI SOGGETTI.....	11
3.1 Il Titolare del trattamento	11
3.2 Soggetti Designati al trattamento	11
3.3 Persone autorizzate al trattamento dei dati personali (art. 29 GDPR)	12
3.4 Responsabile del trattamento dei dati personali (art. 28 GDPR).....	13
3.5 Il Responsabile della protezione dei dati (art. 37 del GDPR).....	13
CAPO IV	14
TRATTAMENTO DEI DATI PERSONALI	14
4.1 Modalità del trattamento.....	14
4.2 Informativa.....	14
4.3. Misure di sicurezza	15
4.3.1 Limiti alla utilizzabilità di dati personali	16
4.4 Conservazione e durata delle registrazioni.....	16
4.5 Sistemi integrati di videosorveglianza	17
CAPO V	17
DIRITTI DEGLI INTERESSATI.....	17
5.1 Diritto di accesso ed altri diritti.....	17

CAPO VI	18
UTILIZZO DI SAPR PER FINALITÀ DI VIDEOSORVEGLIANZA	18
CAPO VII	19
PRIVACY BY DESIGN E BY DEFAULT (ART. 25 GDPR).....	19
CAPO VIII	19
REGISTRO DELLE ATTIVITÀ DEL TRATTAMENTO (ART. 30 GDPR).....	19
CAPO IX	19
DATA BREACH (ART. 33 -34 GDPR).....	19
9.1 Notifica di una violazione dei dati personali all’Autorità Garante (art. 33 GDPR)	19
9.2 Comunicazione di una violazione dei dati personali all’interessato (art. 34 GDPR)	20
CAPO X.....	20
DPIA (ART. 35) E CONSULTAZIONE PREVENTIVA (ART. 36 GDPR).....	20
10.1 DPIA - Valutazione d’impatto sulla protezione dei dati (art. 35 GDPR).....	20
10.2 Consultazione preventiva (art. 36).....	21
CAPO XII	21
CESSAZIONE DEL TRATTAMENTO DEI DATI PERSONALI	21
CAPO XIII	22
TUTELA AMMINISTRATIVA E GIURISDIZIONALE	22
CAPO XIV	22
MODIFICHE AL PRESENTE REGOLAMENTO	22
CAPO XV	22
DISPOSIZIONI FINALI.....	22
15.1 Entrata in vigore del presente Regolamento.....	22
15.2 Rinvio.....	22
15.3 Norme abrogate.....	22
15.4 Pubblicità del presente Regolamento.....	22

CAPO I PRINCIPI GENERALI

1.1 Oggetto

Il presente regolamento ha per oggetto la disciplina delle misure procedurali e regole di dettaglio del trattamento di dati personali, acquisiti mediante sistema di videosorveglianza, affinché ciò si svolga nel rispetto dei diritti, delle libertà fondamentali, della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

Attività quali la raccolta, registrazione, conservazione e, in generale, utilizzo di immagini rappresentano dei trattamenti di dati personali ogni qualvolta abbiano ad oggetto una qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

Il Comune di Noragugume, in qualità di **Titolare** del trattamento, può trattare dati personali nel rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi e soltanto per lo svolgimento delle proprie funzioni istituzionali.

Le prescrizioni del presente Regolamento si fondano sui principi applicabili al trattamento di dati personali quali quello di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza richiamati dall'art. 5 del Regolamento europeo 2016/679 (GDPR) e dal Codice della privacy (D.lgs. 196/03 come modificato dal D.lgs. 101/2018).

1.2 Ambito di applicazione e principi generali

Il regolamento disciplina il trattamento di dati personali, realizzato mediante sistema di videosorveglianza, attivato nel territorio del Comune di Noragugume.

L'utilizzo del sistema della videosorveglianza è attuato attraverso il corretto impiego delle applicazioni e nel rispetto dei principi di cui all'art. 5, Regolamento UE Generale sulla protezione dei dati personali 2016/679 (di seguito GDPR), ovvero:

principio di liceità: il Comune di Noragugume, in ossequio al principio di liceità, prevede che il trattamento di dati personali ottenuti a mezzo dei sistemi di videosorveglianza venga effettuato esclusivamente per lo svolgimento delle funzioni istituzionali e nel rispetto dei presupposti e dei limiti stabiliti dal GDPR e dal Codice della privacy (D.lgs. 196/03 come modificato dal D.lgs. 101/2018), anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.

Principio di adeguatezza: il trattamento dei dati personali è pertinente e limitato a quanto necessario rispetto alle finalità per il quale sono trattati.

Principio di necessità: in ossequio al principio di necessità ogni attività di trattamento dei dati personali acquisiti mediante gli impianti di videosorveglianza non può eccedere la soglia necessaria al raggiungimento degli scopi prefissi nel rispetto delle funzioni istituzionali. La predisposizione degli impianti di videosorveglianza, in sostanza, non può rappresentare di per sé un'esigenza dell'amministrazione comunale, ma deve essere preordinata al soddisfacimento di bisogni specifici.

Principio di proporzionalità: nel commisurare la necessità del sistema di videosorveglianza al 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 una effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. La proporzionalità va valutata in ogni fase o modalità del trattamento.

Principio di finalità: nel rispetto del principio di limitazione della finalità, limitazione della conservazione e di minimizzazione dei dati si prevede che tutte le fasi dell'attività di videosorveglianza siano improntate ad un trattamento di dati personali pertinenti e non eccedenti rispetto alle finalità perseguite dal Comune di Noragugume nell'ambito dello svolgimento delle funzioni istituzionali. Tale principio influenza l'Amministrazione comunale sin dalla scelta delle funzionalità e delle caratteristiche delle telecamere da installare nell'ambito del territorio urbano o della individuazione del numero degli incaricati del trattamento dei dati.

Il principio di limitazione del trattamento, sopra richiamato, nonché quello di correttezza e trasparenza, prevedono che gli scopi del trattamento siano legittimi (il soggetto che esegue il trattamento deve essere legittimato al perseguimento delle finalità del trattamento), determinati ed espliciti (ossia predeterminati e comunicati, mediante idonea informativa, agli eventuali interessati al trattamento).

Per tutto quanto non disciplinato dal presente Regolamento si rinvia alle disposizioni del Regolamento Europeo (UE) 2016/679, del Codice della privacy (D.lgs. 196/2003 come modificato dal D.lgs. 101/2018) e al provvedimento del Garante Privacy in materia di videosorveglianza del 8 aprile 2010.

Principio di pertinenza e non eccedenza: il sistema informativo e i programmi informatici (di cui al trattamento dei dati personali) 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.

Il trattamento dei dati personali riferito agli ambiti cui si riferisce il regolamento non necessita del consenso degli interessati in quanto viene effettuato per lo svolgimento di funzioni che sono assoggettate ad un regime di tipo particolare.

1.3 Definizioni

Ai fini del presente Regolamento si intende per:

- a) **“dato personale”**, qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- b) **“trattamento”**, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- c) **“Titolare”**, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il **Titolare** del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri. Ai fini del presente Regolamento il **Titolare** del trattamento dei dati personali è il Comune di Noragugume;

- d) **“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 ai sensi dell'art. 28 del GDPR;
- e) **“Designato”**, la persona fisica e qualsiasi altro ente, associazione od organismo istruiti e autorizzati dal **Titolare** al trattamento di dati personali, nel rispetto delle disposizioni di cui all'art. 2-quaterdecies del Codice della privacy;
- f) **“autorizzato”**, la persona fisica istruita e autorizzata a compiere operazioni di trattamento dal **Titolare** o dal **responsabile** interno, nel rispetto delle disposizioni di cui all'art. 2-quaterdecies del Codice della privacy e art. 29 GDPR.
- g) **“interessato”**, la persona fisica cui si riferiscono i dati personali;
- h) **“banca dati”**, il complesso di dati personali, formatosi presso la sala di controllo e trattato esclusivamente mediante riprese video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto utilizzati dagli stessi soggetti;
- i) **“comunicazione”**, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del **Titolare** nel territorio dell'Unione europea, dal **responsabile** o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate (ai sensi dell'articolo 2-quaterdecies del Codice della privacy) al trattamento dei dati personali sotto l'autorità diretta del **Titolare** o del **responsabile**, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
- l) **“diffusione”**, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- m) **“dato anonimo”**, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- n) **“blocco”**, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.
- o) **“misure tecniche e organizzative”**, il complesso delle misure tecniche e organizzative di cui all'art. 32 del GDPR.

1.4 Normativa di riferimento

Il presente Regolamento tiene conto oltre che del Codice per il trattamento dei dati personali, il (D.lgs. 196/2003 come modificato dal D.lgs 101/2018), anche delle norme di cui al Regolamento Europeo (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (pubblicato nella Gazzetta ufficiale dell'Unione europea L.119 del 4 maggio 2016) che trova applicazione a decorrere dal 25 maggio 2018.

Rilevante, in materia, è anche il provvedimento del Garante privacy in materia di videosorveglianza datato 8 aprile 2010, il quale prescrive ai titolari del trattamento di dati personali effettuato tramite sistemi di videosorveglianza, di adottare particolari misure e accorgimenti concernenti, tra gli altri, gli obblighi di: rendere l'informativa visibile anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno; di sottoporre i trattamenti che presentano rischi specifici per i diritti e le libertà fondamentali degli interessati, alla valutazione d'impatto di cui al capo IV, sezione 3 del GDPR; di adottare le misure di sicurezza a protezione dei dati registrati tramite impianti

di videosorveglianza e di adottare le misure necessarie per garantire il rispetto di quanto indicato a proposito di utilizzo condiviso dei sistemi di videosorveglianza.

Nella redazione del presente Regolamento, inoltre, si è tenuto conto delle linee guida Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video adottate il 29.01.2020, delle informazioni contenute nelle linee guida ANCI per i Comuni in materia di videosorveglianza; della Circolare Min. Interno n. 558/A/421.2/70 e di quella n. 558/A/421.2/70/195960 del 6 agosto 2010. Per quanto riguarda, inoltre, la interconnessione, a livello territoriale, delle sale operative della polizia locale con le sale operative delle forze di polizia e la regolamentazione dell'utilizzo in comune di sistemi di sicurezza tecnologica finalizzati al controllo delle aree e delle attività soggette a rischio dovranno considerarsi le linee generali delle politiche pubbliche per la promozione della sicurezza integrata, adottate ai sensi dell'art. 2 del D.L. 20 febbraio 2017, n. 14, (cd. Decreto sicurezza), convertito con modifiche nella Legge 18 aprile 2017, n. 48, recante *"Disposizioni urgenti in materia di sicurezza delle città"*.

Ancora per la prevenzione e repressione dei reati, trova applicazione la Direttiva (UE) 2016/680 e il D.lgs. 51/2018, che ne disciplina il recepimento. Bisogna evidenziare come detta Direttiva abbia natura di *lex specialis* rispetto al Regolamento generale sulla protezione dei dati, di cui declina principi e obblighi con riguardo allo specifico contesto di attività e ai poteri delle autorità di polizia e giudiziarie. Il D.lgs. 51/2018, regola il trattamento dei dati personali per finalità di prevenzione e repressione di reati, esecuzione di sanzioni penali, salvaguardia contro le minacce alla sicurezza pubblica e prevenzione delle stesse, da parte sia dell'autorità giudiziaria, sia delle forze di polizia.

CAPO II FINALITÀ DEL TRATTAMENTO

2.1 Finalità del trattamento

Il trattamento dei dati, conforme alle finalità istituzionali demandate al Comune di Noragugume, ed in particolare sul territorio comunale, attraverso l'acquisizione di dati ed immagini, si espleta tramite:

- a) **monitoraggio del traffico.** In particolare: monitoraggio delle arterie stradali a maggiore rilevanza nel territorio, a fini di prevenzione di problemi inerenti i flussi veicolari e la mobilità stradale, vigilanza del traffico ed individuazione dei luoghi ad elevata intensità, che impongono il pronto intervento della Polizia Locale.
- c) **sicurezza urbana.** Protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, l'ordine e la sicurezza pubblica, la prevenzione, accertamento o repressione dei reati, la razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti;
- d) **tutela degli immobili di proprietà o in gestione dell'Amministrazione Comunale e prevenzione di eventuali atti di vandalismo o danneggiamento;**
- e) **controllo 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;
- f) **rilevazione e accertamento delle violazioni dei Regolamenti e ordinanze comunali;**
- g) **acquisire elementi probatori in fattispecie di violazioni amministrative o penali;**
- h) **attivare uno strumento operativo di protezione civile sul territorio comunale;**

i) **tutela dell'ordine e della sicurezza pubblica**, prevenzione, accertamento o repressione dei reati. Si precisa che quest'ultima finalità è soggetta alla speciale disciplina dettata dalla Direttiva 2016/680/UE e dal D.lgs 51/2018.

Ai sensi di quanto previsto dall'articolo 4 della Legge 20 maggio 1970, n. 300, così come modificato dal D.lgs. 151/2015 e dal D.lgs. 185/2016, gli impianti di videosorveglianza non possono essere utilizzati, salvi i casi previsti dal medesimo articolo, per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

Il sistema di videosorveglianza comporterà esclusivamente il trattamento di dati personali rilevati mediante le riprese della videosorveglianza e che, in relazione ai luoghi di installazione delle videocamere, interesseranno i soggetti ed i mezzi di trasporto, che transiteranno nell'area interessata e comunque solo i dati strettamente necessari per il raggiungimento delle finalità perseguite.

2.1 1 Monitoraggio del traffico

I sistemi di videosorveglianza possono essere impiegati al fine di monitorare le condizioni e il flusso del traffico nell'ambito urbano. I sistemi di videosorveglianza, quando impiegati esclusivamente per le finalità di monitoraggio del traffico, nel rispetto del principio di necessità sono configurati in modo da ridurre al minimo il trattamento di dati personali, ad esempio riducendo la definizione delle immagini in modo tale da non rendere riconoscibili i volti delle persone o le targhe delle autovetture ovvero limitando le funzioni di zoom delle telecamere brandeggiabili.

2.1 2 Sicurezza urbana

Il Comune di Noragugume gestisce gli impianti di videosorveglianza anche per finalità di sicurezza urbana. A tal proposito si richiama la definizione di sicurezza urbana quale *“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”* di cui al Decreto Min. Interno 5 agosto 2008.

Tutte le operazioni di videosorveglianza per finalità di sicurezza urbana e di prevenzione e repressione degli atti delittuosi, delle attività illecite e degli episodi di microcriminalità commessi sul territorio comunale e quindi, sostanzialmente orientate ad assicurare maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di *“sicurezza urbana”*, devono essere funzionali rispetto ai compiti affidati al Comune di Noragugume.

Le immagini, per tali finalità, potranno essere visionate e gestite:

- sulla base di denunce di atti criminosi da parte dei cittadini, per il successivo inoltro delle eventuali fonti di prova all'autorità giudiziaria;
- sulla base di segnalazioni relative ad atti criminosi accertate direttamente dagli organi di polizia in servizio sul territorio cittadino;
- 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;
- sulla base di richieste specifiche per indagini da parte dell'autorità giudiziaria;
- sulla base di ogni altra richiesta di specifici organi/autorità che siano espressamente autorizzati, secondo specifiche norme di legge.

A tal fine le immagini sono custodite nel rispetto delle misure tecniche e organizzative adeguate, di cui all'art. 32 del GDPR, anche al fine di impedire trattamenti non autorizzati (confidenzialità, integrità e disponibilità dei dati). Altre eventuali future postazioni attraverso le quali accedere, da remoto, ai sistemi di videosorveglianza per finalità di sicurezza urbana, dovranno prevedere, per le medesime finalità di sicurezza, modalità di accesso tali da escludere qualsivoglia trattamento a soggetti non incaricati espressamente.

Della estrapolazione di immagini o di registrazione di sequenze audio/video degli impianti di videosorveglianza è tenuta idonea documentazione. L'accesso ai server in cui sono custodite le registrazioni o i pannelli di controllo degli impianti di videosorveglianza sono condizionati ad un'autenticazione di cui il sistema deve tenere evidenza.

La registrazione delle immagini raccolte al fine di soddisfare le finalità di cui al presente articolo sono conservate per un massimo di 7 giorni successivi all'acquisizione. Qualora eventuali esigenze particolari dovessero richiedere un tempo superiore di conservazione il Comune di Noragugume dovrà preliminarmente eseguire una valutazione di impatto o procedere alla consultazione preventiva con l'Autorità Garante sancita dall'art. 36 GDPR.

In tutte le ipotesi in cui il trattamento dei dati personali ottenuti in conseguenza delle **attività di videosorveglianza avvenga per finalità di polizia**, ovvero siano direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati, trova applicazione la Direttiva (UE) 2016/680 e il D.lgs. 51/2018 che ne disciplina il recepimento. In considerazione dell'applicazione della Direttiva 2016/680 viene meno, tra l'altro, l'obbligo di prestare idonea informativa per le singole telecamere degli impianti di videosorveglianza.

2.1.3 Abbandono di rifiuti e vigilanza ambientale

Gli impianti di videosorveglianza **possono** essere utilizzati dal Comune di Noragugume previa prestazione di idonea informativa riportante tale finalità, per il monitoraggio di ipotesi di utilizzo abusivo di aree come discariche di materiali e di sostanze pericolose e solo nei casi in cui non sia possibile o risulti inefficace il ricorso ad altri strumenti e sistemi di controllo.

Gli impianti di videosorveglianza possono altresì essere utilizzati dal Comune di Noragugume previa prestazione di **idonea informativa riportante tale finalità**, per il monitoraggio del rispetto delle regole circa modalità, tipologia ed orario di deposito dei rifiuti la cui violazione sia sanzionata amministrativamente, nei casi in cui non sia possibile o risulti inefficace il ricorso ad altri strumenti e sistemi di controllo.

2.1.4 Body cam e dash cam

Gli operatori di Polizia Locale **possono** utilizzare, per i servizi a maggior rischio operativo, delle Body Cam (telecamere sull'operatore) e delle Dash Cam (telecamere a bordo dei veicoli di servizio) in conformità alle indicazioni contenute nella nota 26 luglio 2016, prot. n. 49612 del Garante della Privacy, con la quale sono state impartite le prescrizioni generali di utilizzo dei predetti dispositivi. L'utilizzo di tali dispositivi rientra nell'ambito di applicazione del D.lgs 51/2018.

Il Comando del Corpo curerà la predisposizione di uno specifico disciplinare tecnico interno, da somministrare agli operatori di Polizia Municipale che saranno dotati di microcamere, con specificazione dei casi in cui le microcamere devono essere attivate, dei soggetti eventualmente

autorizzati a disporre l'attivazione (ad es. il capo-pattuglia), delle operazioni autorizzate nel caso di emergenza e di ogni altra misura organizzativa e tecnica necessaria alla corretta e legittima gestione di detti dispositivi.

Le videocamere e le schede di memoria di cui sono dotati i sistemi di cui ai commi precedenti dovranno essere dotate di un numero seriale da annotarsi in registro, recante il giorno, l'orario, i dati indicativi del servizio e la qualifica e nominativo del dipendente.

La scheda di memoria, all'atto della consegna ai singoli operatori, non dovrà contenere alcun dato archiviato.

Il sistema di registrazione dovrà essere attivato solo in caso di effettiva necessità, per i servizi a maggior rischio operativo. L'ordine di attivazione e di disattivazione del dispositivo deve essere emesso dall'Ufficiale di Polizia Giudiziaria che impiega direttamente la pattuglia o, in mancanza, dalla Centrale Operativa.

Al termine del servizio gli operatori interessati, previa compilazione di un foglio di consegna, affideranno tutta la documentazione video realizzata all'Ufficiale **responsabile**, il quale provvederà alla sua consegna al Comando.

2.1.5 Telecamere modulari (fototrappole)

Potranno essere posizionate, su tutto il territorio comunale, delle telecamere modulari (foto trappole) con generazione di allarmi da remoto per il monitoraggio attivo.

Le telecamere modulari mobili dovranno essere utilizzate esclusivamente nei luoghi teatro di illeciti penali o amministrativi, e, in quest'ultimo caso, esclusivamente nelle ipotesi in cui non sia possibile o risulti inefficace il ricorso ad altri strumenti e sistemi di rilevazione. Qualora non sussistano necessità di indagine previste dal D.lgs 51/2018 che esimono il **Titolare** dall'obbligo di informazione, si provvederà alla previa collocazione della adeguata cartellonistica, per l'informativa agli utenti frequentatori di dette aree.

2.1.6 Istituti scolastici

Il sistema di videosorveglianza attivo presso istituti scolastici, nel rispetto di quanto previsto dal paragrafo 4.3 del provvedimento del Garante Privacy in materia di videosorveglianza del 8 aprile 2010, dovrà garantire il diritto dello studente alla riservatezza, prevedendo opportune cautele al fine di assicurare l'armonico sviluppo delle personalità dei minori in relazione alla loro vita, al loro processo di maturazione ed al loro diritto all'educazione.

In tale quadro, potrà risultare ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate ed attivando gli impianti negli orari di chiusura degli istituti. È vietato, altresì, attivare le telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche, che si svolgono all'interno della scuola.

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

CAPO III

RUOLI E COMPITI DEI SOGGETTI

3.1 Il Titolare del trattamento

Il Comune di Noragugume è **Titolare** del trattamento dei dati personali (art. 4, comma 1, n. 7 GDPR) acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento. A tal fine al Comune di Noragugume, anche unitamente ad altro **Titolare (contitolare)**, compete ogni decisione in ordine alle finalità e modalità del trattamento, agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Per tale ragione, il **Titolare** del trattamento dei dati personali:

- a) definisce le linee organizzative per l'applicazione della normativa di settore;
- b) qualora un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il **Titolare** deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali, di seguito indicata con "DPIA", ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, e, ove necessario, la consultazione preventiva ex. art. 36 GDPR;
- c) nomina i **designati** e gli **autorizzati** per la gestione tecnica degli impianti di videosorveglianza ed i responsabili del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza, impartendo istruzioni ed assegnando compiti e responsabilità;
- d) nomina quale **Responsabile del trattamento**, soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;
- e) allorché due o più **Titolari** determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD.
- f) detta le linee guida di carattere fisico, logico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza;
- g) vigila sulla puntuale osservanza delle disposizioni impartite;
- h) comunica all'**Autorità Garante** le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali.

3.2 Soggetti Designati al trattamento

Il Comune di Noragugume, nella sua qualità di **Titolare** del trattamento dei dati personali acquisiti a seguito delle attività di videosorveglianza disciplinate dal presente Regolamento, fatti salvi i casi in cui trovi applicazione la disciplina speciale di cui alla Direttiva 2016/680/UE e al D.lgs 51/2018, designa per iscritto uno o più soggetti, che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. La designazione è fatta per iscritto con indicazione analitica dei compiti affidatigli. In particolare sono disciplinati:

- a) la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- b) il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- c) gli obblighi ed i diritti del **Titolare** del trattamento.

Il **Designato** al trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

Il **Designato** al trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal **Titolare**, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:

- ✓ all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- ✓ alla sensibilizzazione e formazione del personale, che partecipa ai trattamenti ed alle connesse attività di controllo;
- ✓ ad assistere il **Titolare** nella conduzione della valutazione dell'impatto sulla protezione dei dati, di seguito indicata con "*DPIA*", fornendo allo stesso ogni informazione di cui è in possesso;
- ✓ informare il **Titolare**, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione al Garante Privacy, nel caso che il **Titolare** stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati;

Il **Designato** al trattamento ha l'onere di custodire le chiavi per l'accesso a locali e/o ove sono custoditi i servers, nonché le password per l'accesso ed utilizzo dei sistemi informatici.

Tra i designati al trattamento viene individuato il **Responsabile del servizio di Polizia Locale** per le telecamere collegate al Servizio di Polizia Locale.

3.3 Persone autorizzate al trattamento dei dati personali (art. 29 GDPR)

Il **Designato** individua e nomina, gli **autorizzati alla gestione dell'impianto** nel numero ritenuto sufficiente a garantire il corretto funzionamento del servizio di videosorveglianza, che per esperienza, capacità ed affidabilità forniscono idonea garanzia nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati; inoltre conferisce incarico a tutti gli operatori che in via principale o residuale effettuano o dovranno effettuare un trattamento dei dati. In tal modo, le operazioni di trattamento di dati personali possono essere effettuate esclusivamente dalle persone autorizzate al trattamento dal **Titolare** o dal **Designato**, per iscritto con atto di designazione riportante la individuazione puntuale e analitica le istruzioni da seguire nell'ambito del trattamento consentito.

Nell'atto di designazione sono analiticamente indicate, tra le altre, la possibilità di accedere ai locali ove siano situate le postazioni di controllo della videosorveglianza; l'eventuale possibilità di utilizzare gli impianti, di visionare le immagini, di copiare o stampare le immagini, di gestire le registrazioni; vengono definite le istruzioni in tema di misure di sicurezza e si individuano gli specifici livelli di accesso consentiti in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore.

Fra coloro che rivestono la qualifica di **persona autorizzata al trattamento**, con l'atto di nomina verranno individuati i soggetti cui è affidata la custodia e conservazione delle password e delle chiavi di accesso alla sala operativa.

3.4 Responsabile del trattamento dei dati personali (art. 28 GDPR)

Nelle ipotesi in cui il Comune di Noragugume affidi la gestione o la manutenzione degli impianti di videosorveglianza a un soggetto esterno all'amministrazione comunale, quest'ultimo deve considerarsi **Responsabile del trattamento** dei dati personali e il relativo rapporto deve essere regolato da un contratto o altro atto negoziale conforme all'art. 28 del GDPR.

1. Il **Responsabile** deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

2. Il **Responsabile** del trattamento dei dati personali dovrà:

- a) organizzare il trattamento delle immagini registrate e/o visualizzate tramite i sistemi di videosorveglianza;
- b) nominare per iscritto gli incaricati del trattamento dei dati e delle immagini in presenza di differenti competenze specificatamente attribuite ai singoli operatori;
- c) controllare che il periodo di conservazione delle immagini sia conforme a quanto previsto dalla normativa vigente;
- d) vigilare sulla puntuale osservanza, da parte delle persone autorizzate al trattamento, delle istruzioni impartite e sul corretto svolgimento dei trattamenti di propria competenza;
- e) verificare e controllare che il trattamento dei dati effettuato mediante sistema di videosorveglianza, sia realizzato nel rispetto dei principi di cui all'articolo 5 del GDPR e, in particolare, assicurare che i dati personali siano trattati in modo lecito, corretto e trasparente;
- f) garantire altresì che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità.

3. Il **Responsabile** non può ricorrere ad altro **Responsabile** senza autorizzazione scritta, specifica o generale da parte del **Titolare** del trattamento.

4. Il **Responsabile** del trattamento, tenuto conto del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, adotta tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del GDPR.

5. Il **Responsabile** deve assistere il **Titolare** ai fini di soddisfare le richieste di esercizio dei diritti da parte dell'interessato, nell'adempimento degli obblighi di sicurezza (art. 32), nella notificazione delle violazioni di dati personali (artt. 33-34), nella valutazione d'impatto sulla protezione dei dati (art. 35) e nella consultazione preventiva (art. 36).

6. Il **Responsabile** deve, a scelta del **Titolare**, cancellare o restituire tutti i dati personali, una volta terminata la prestazione del servizio.

3.5 Il Responsabile della protezione dei dati (art. 37 del GDPR)

Il **Responsabile** della protezione dei dati, **Designato** ai sensi dell'art. 37 del GDPR, deve essere tempestivamente e adeguatamente coinvolto nelle questioni riguardanti i trattamenti per finalità di videosorveglianza.

In particolare, il **Responsabile** della protezione dei dati:

- a) può essere contattato dagli interessati, anche con riguardo ai trattamenti per finalità di videosorveglianza;
- b) deve svolgere attività di consulenza sui trattamenti, anche a favore dei dipendenti che effettuano il trattamento;

- c) deve sorvegliare l'osservanza delle norme in tema di protezione di dati personali, nonché del presente Regolamento, e deve verificare l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale incaricato;
- d) deve fornire se richiesto un parere sulla valutazione d'impatto sulla protezione dei dati, di cui all'art 35 del GDPR e dal presente Regolamento;
- e) deve cooperare con l'Autorità Garante e fungere da punto di contatto.

CAPO IV

TRATTAMENTO DEI DATI PERSONALI

4.1 Modalità del trattamento

Il presente **Regolamento** assicura che il trattamento dei dati personali acquisiti mediante gli impianti di videosorveglianza gestiti dal Comune di Noragugume si svolga nel pieno rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche.

I dati raccolti dall'Ente, tramite l'impianto di videosorveglianza, sono quelli strettamente necessari per il raggiungimento delle finalità istituzionali perseguite, attraverso la registrazione delle sole immagini indispensabili, la limitazione dell'angolo visuale delle riprese e l'estensione, se non strettamente necessario, dall'effettuazione di riprese dettagliate e/o ingrandite nel rispetto dei principi di cui all'art. 5 del GDPR.

Il **Titolare** del trattamento non effettuerà riprese dettagliate dei tratti somatici dei soggetti, se non gli stessi dovessero essere funzionali rispetto alle finalità perseguite, nonché alle funzioni istituzionali e di interesse pubblico per le quali l'impianto di videosorveglianza è stato attivato.

Le attività di controllo dei sistemi di videosorveglianza avvengono prevalentemente presso la centrale operativa del Comune di Noragugume e ciò, in particolare, per quanto riguarda gli impianti di videosorveglianza relativi al monitoraggio del traffico, rilevazione delle infrazioni al codice della strada. In questi ambiti di operatività degli impianti di videosorveglianza le comuni operazioni di gestione, visualizzazione, interconnessione, registrazione e controllo degli impianti di videosorveglianza avviene presso la suddetta centrale operativa.

Presso la medesima sede si trova anche l'impianto centralizzato per la tutela della sicurezza urbana, basato su tecnologia IP che, tuttavia, consente nel rispetto delle norme sul trattamento dei dati personali anche l'accesso remoto, tramite personale espressamente autorizzato all'accesso, alla gestione e alle operazioni sui dati (in streaming o memorizzati dal sistema).

Dietro specifico provvedimento o accordo con l'Autorità Giudiziaria o con la Polizia Giudiziaria può fornirsi la possibilità a questi ultimi di eseguire operazioni quali l'accesso, la visualizzazione in diretta o in differita, l'accesso alle registrazioni audiovisive o alla stessa possibilità di eseguire le registrazioni in autonomia, anche mediante l'interconnessione, attraverso reti dedicate o reti pubbliche previa cifratura delle connessioni al fine di evitare che terzi possano intercettare in tutto o in parte il flusso di dati, con la centrale operativa del Comune di Noragugume

4.2 Informativa

Fatti salvi i trattamenti le cui finalità comportino l'applicazione della **Direttiva 2016/680/UE** e del **D.lgs 51/2018** (che rendono facoltativa la prestazione dell'informativa sul trattamento dei dati personali), il Comune di Noragugume fornisce agli interessati, che accedono o transitano in luoghi ove siano attivi sistemi di videosorveglianza, un'idonea informativa mediante apposita

cartellonistica, contenente un modello di nota informativa semplificata minima e indicante i dati individuati dalle **Linee Guida 3/2019** sul trattamento dei dati personali attraverso dispositivi video del **Comitato Europeo** per la protezione dei dati personali, adottate il 29.01.2020.

L'informativa ha lo scopo di avvisare gli interessati, che stanno per accedere in una zona videosorvegliata e deve essere collocata prima del raggio d'azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti. L'informativa deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno e può inglobare un simbolo o una stilizzazione di esplicita ed immediata comprensione al fine di informare se le immagini sono solo visionate o anche registrate.

L'informativa "minima" (***informativa di primo livello***), riporta l'indicazione del **Titolare** del trattamento e delle finalità del trattamento e può recare al suo interno un collegamento (ipertestuale, QR-code o altro) all'informativa completa (***informativa di secondo livello***) e contenente tutti gli elementi previsti dall'art. 13 del GDPR.

L'informativa può non essere resa quando i dati personali sono trattati per il perseguimento delle finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati e nelle ipotesi previste dalla **Direttiva 2016/680/UE e dal D.lgs 51/2018**.

4.3. Misure di sicurezza

I dati raccolti mediante sistemi di videosorveglianza dal **Comune di Noragugume** sono protetti con misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato, per ridurre al minimo i rischi 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, anche in relazione alla trasmissione delle immagini (art. 32 del GDPR).

Le misure di sicurezza garantiscono:

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

Sono adottate specifiche misure tecniche ed organizzative che consentono al **Titolare** di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa.

In particolare, le misure di sicurezza devono rispettare i seguenti principi:

- in presenza di differenti competenze specificatamente attribuite ai singoli operatori sono configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati o autorizzati al trattamento, devono essere in possesso di **credenziali di autenticazione**, che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;
- per i sistemi configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente valutata la possibilità, per i soggetti espressamente abilitati, di

visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;

- per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;
- nel caso di interventi derivanti da esigenze di manutenzione, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
- la trasmissione tramite una rete pubblica di comunicazione o tramite sistemi wireless di immagini, riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche, che ne garantiscano la riservatezza;
- ciascun sistema informativo ed il relativo programma informatico vengono conformati già in origine in modo da non utilizzare dati relativi a persone identificabili, quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (ad esempio con riferimento alle finalità esclusive di monitoraggio del traffico).

4.3.1 Limiti alla utilizzabilità di dati personali

L'utilizzabilità dei dati trattati è vincolata alla finalità per cui essi sono raccolti e non potranno essere utilizzati per finalità diverse se non per quelle direttamente connesse e consequenziali alle finalità che ne legittima la raccolta.

4.4 Conservazione e durata delle registrazioni

Nell'ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, il termine massimo di durata della conservazione delle informazioni e delle immagini è limitato ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione.

In merito, il paragrafo 3.4 del Prov. 08.04.2010 afferma che per i Comuni, e nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, il termine massimo di durata della conservazione dei dati sia limitato *"ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione"*.

Il provvedimento richiama, l'art. 6, co. 8, del D.L. 23/02/2009, n. 11, ai sensi del quale, nell'ambito dell'utilizzo da parte dei Comuni di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana, *"la conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione"*.

Sono, altresì, impiegate misure tecniche o organizzative al fine di operare l'integrale cancellazione, anche in modalità automatizzata mediante sovra-registrazione delle informazioni allo scadere del termine previsto. Il sistema di cancellazione deve rendere non riutilizzabili i dati cancellati. In presenza di impianti basati su tecnologia non digitale la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal **Titolare**.

Ne segue che le speciali esigenze di ulteriore conservazione oltre il termine di sette giorni di cui al sopra sono precedute, ove necessario, da una valutazione d'impatto ex art. 35 GDPR o da una consultazione preventiva con l'Autorità Garante ex art. 36 GDPR, a meno che non derivi da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso.

4.5 Sistemi integrati di videosorveglianza

Nell'ambito dei trattamenti mediante sistemi integrati di videosorveglianza tra il Comune di Noragugume ed altri soggetti pubblici, mediante gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento, che utilizzano le medesime infrastrutture tecnologiche, i singoli titolari possono trattare le immagini nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali ed alle finalità chiaramente indicate nell'informativa.

È prevista la possibilità di attivare un collegamento dei sistemi di videosorveglianza comunali con le sale o le centrali operative degli organi di polizia. L'attivazione del predetto collegamento deve essere reso noto agli interessati mediante l'informativa, salvo i casi di informativa facoltativa ai sensi del D.lgs 51/2018.

Tali modalità di trattamento richiedono l'adozione delle seguenti misure di sicurezza ulteriori:

- 1) adozione di sistemi idonei alla registrazione degli accessi degli autorizzati 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 e degli autorizzati da parte del **Titolare**, comunque non inferiore a sei mesi;
- 2) separazione logica dei trattamenti di dati personali effettuati dai diversi titolari in relazione alle competenze istituzionali di ciascuna amministrazione.

L'utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell'ente.

CAPO V DIRITTI DEGLI INTERESSATI

5.1 Diritto di accesso ed altri diritti

I soggetti a cui si riferiscono i dati personali possono esercitare in qualsiasi momento i diritti sanciti dagli artt. 15-22 GDPR, ferme restando le eccezioni previste per le Amministrazioni pubbliche nelle ipotesi di esercizio di compiti svolti nel pubblico interesse ovvero nell'esercizio di pubblici poteri. Qui di seguito sono riportati i diritti che l'interessato può esercitare con riguardo alla videosorveglianza:

- il diritto di chiedere al **Titolare** l'accesso ai dati personali ed alle informazioni relative agli stessi, la rettifica dei dati inesatti o l'integrazione di quelli incompleti, l'interruzione del trattamento o la cancellazione dei dati personali (al verificarsi di una delle condizioni indicate nell'art. 17, paragrafo 1 del GDPR e nel rispetto delle eccezioni previste nel paragrafo 3 dello stesso articolo, ad esempio se i dati sono trattati illecitamente), la limitazione del trattamento dei dati personali (al ricorrere di

una delle ipotesi indicate nell'art. 18, paragrafo 1 del GDPR, ad esempio i dati sono trattati illecitamente).

- il diritto di opporsi in qualsiasi momento al trattamento dei dati personali, alle condizioni previste dall'art. 21 GDPR.
- il diritto di proporre reclamo a un'Autorità di controllo (Autorità Garante per la protezione dei dati personali - www.garanteprivacy.it), nel caso in cui l'istanza per l'esercizio dei diritti di cui sopra dovesse dare esito negativo, ovvero di rivolgersi all'Autorità Giudiziaria ordinaria.

I suddetti diritti sono esercitabili entro i limiti indicati dall'art. 3.5 del Provvedimento videosorveglianza. In particolare, 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.

Tutti i suddetti diritti potranno essere esercitati mediante richiesta da inoltrarsi al **Titolare** del trattamento, inviando una pec all'indirizzo protocollo@pec.comune.noragugume.nu.it ovvero tramite lettera raccomandata A/R all'indirizzo: Comune di Noragugume, Piazza IV Novembre n. 1. Nell'esercizio dei diritti l'interessato potrà farsi assistere da una persona di fiducia, ovvero conferire delega o procura a persone fisiche, enti o associazioni, organismi, affinché esercitino per suo conto i predetti diritti.

Per ciascuna delle richieste può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese secondo le modalità previste dalla normativa vigente. Non possono, di norma, essere rilasciate copie delle immagini registrate concernenti altri soggetti diversi dall'interessato, salvi casi particolarmente meritevoli di tutela; se le immagini contengono dati riferibili a terzi, l'accesso del richiedente è consentito soltanto se la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi a terzi. Copia delle immagini potranno essere rilasciate all'Autorità Giudiziaria ed alle Forze di Polizia per finalità di indagini giudiziarie, amministrative e risarcimento danni.

A seguito di segnalazione e/o denuncia di fatti rilevanti da un punto di vista giudiziario, amministrativo e risarcitorio il Comando Polizia Locale provvederà ad estrapolare le immagini e a trattarle per le finalità delle indagini di polizia. Tali immagini, che riproducono anche altri dati personali e/o particolari, non potranno mai essere consegnate al segnalante e/o denunciante salvo specifica autorizzazione del Garante della Privacy e dell'Autorità Giudiziaria.

CAPO VI

UTILIZZO DI SAPR PER FINALITÀ DI VIDEOSORVEGLIANZA

I Sistemi aeromobili a pilotaggio remoto (SAPR), comunemente noti come "droni" possono essere utilmente impiegati per integrare i trattamenti per finalità di videosorveglianza.

Il Comune, nei bandi e nei contratti per l'acquisizione dei servizi di videosorveglianza a mezzo SAPR, cura l'inserimento di apposite clausole che garantiscano il rispetto del Regolamento ENAC "mezzi aerei a pilotaggio remoto", applicabile anche ai SAPR utilizzati dagli Enti locali, e dei principi generali in tema di trattamento di dati personali. In particolare, devono essere individuate le responsabilità per la specifica operazione di volo e le eventuali limitazioni e condizioni connesse, anche con

riguardo alle disposizioni in materia di protezione dei dati personali, con precipuo riguardo al rispetto del principio di necessità.

Nel caso in cui si implementino sistemi intelligenti, o sciami di SAPR interconnessi, sarà necessario procedere a una valutazione d'impatto.

CAPO VII

PRIVACY BY DESIGN E BY DEFAULT (ART. 25 GDPR)

Con l'art. 25 GDPR si sancisce l'effettiva attuazione dei principi di protezione dei dati e dei diritti e delle libertà degli interessati fin dalla progettazione e per impostazione predefinita.

Ciò richiede che i Titolari del trattamento attuino misure tecniche e organizzative adeguate per proteggere i diritti e le libertà degli interessati. I Titolari del trattamento devono essere in grado di dimostrare l'efficacia delle misure attuate e al momento della determinazione delle modalità del trattamento che i titolari del trattamento devono attuare misure e garanzie progettate per attuare efficacemente i principi di protezione dei dati.

Il Comune dovrà, sia per gli impianti di nuova adozione, sia per gli impianti esistenti, accertare il rispetto dei principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita.

In particolare, prima di procedere al trattamento, dovranno essere adottate:

1. misure tecniche e organizzative adeguate, volte ad attuare i principi del GDPR e integrare nel trattamento le necessarie garanzie e tutelare i diritti degli interessati;
2. misure tecniche e organizzative adeguate, volte a garantire che siano trattati, per impostazione predefinita, soltanto i dati necessari per ogni specifica finalità, con particolare riguardo alla quantità dei dati raccolti, alla portata del trattamento, al periodo di conservazione e all'accessibilità ai dati.
3. procedere con l'elaborazione di una valutazione d'impatto ai sensi dell'art. 35 GDPR.

CAPO VIII

REGISTRO DELLE ATTIVITÀ DEL TRATTAMENTO (ART. 30 GDPR)

Il Comune, in sede di redazione e aggiornamento del Registro delle attività di trattamento di cui all'art. 30 GDPR, cura che siano correttamente riportati e adeguatamente descritti i trattamenti effettuati per finalità di videosorveglianza, con particolare riguardo alle finalità del trattamento, alle categorie degli interessati, alle categorie di dati personali, ai termini previsti per la cancellazione, e alle misure di sicurezza tecniche e organizzative adottate ai sensi dell'art. 32 GDPR.

Il Comune verifica che gli eventuali Responsabili nominati ai sensi dell'art. 28 del GDPR adottino a loro volta il Registro delle attività di trattamento, ai sensi dell'art. 30, comma II del GDPR.

CAPO IX

DATA BREACH (ART. 33 -34 GDPR)

9.1 Notifica di una violazione dei dati personali all'Autorità Garante (art. 33 GDPR)

Il Comune, in caso di violazione dei dati personali, deve notificare la violazione all'Autorità Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a

conoscenza. Qualora la notifica non sia effettuata entro tale termine, essa deve indicare anche i motivi del ritardo.

La notifica non deve essere effettuata se è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

La notifica contiene quantomeno:

- a) la descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di record interessati;
- b) la comunicazione del nome e dei dati di contatto del **responsabile** della protezione dei dati;
- c) la descrizione delle probabili conseguenze della violazione e delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e/o per attenuarne i possibili effetti negativi.

Indipendentemente dalla notificazione o comunicazione, il Comune deve documentare qualsiasi violazione dei dati personali, specificando le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, e conservare la relativa documentazione.

9.2 Comunicazione di una violazione dei dati personali all'interessato (art. 34 GDPR)

Il Comune, in caso di violazione dei dati personali, suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, deve comunicare la violazione agli interessati, senza ritardo.

La comunicazione deve essere redatta in linguaggio semplice e chiaro, e deve contenere:

- la descrizione della natura della violazione;
- la comunicazione del nome e dei dati di contatto del **responsabile** della protezione dei dati;
- la descrizione delle probabili conseguenze della violazione e delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e/o per attenuarne i possibili effetti negativi.

La comunicazione non è dovuta qualora:

1. si siano adottate misure tecniche e organizzative adeguate di protezione, applicate ai dati personali oggetto della violazione, con particolare riguardo alle misure destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
2. vengano successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
3. la comunicazione richiederebbe sforzi sproporzionati. In tal caso, il Comune procederà tramite comunicazione pubblica o misura simile, quale pubblicazione sul sito istituzionale, annunci sulle pagine social, comunicati stampa e pubblicazione di annunci a pagamento per un termine congruo al fine di informare gli interessati con analoga efficacia.

CAPO X

DPIA (ART. 35) E CONSULTAZIONE PREVENTIVA (ART. 36 GDPR)

10.1 DPIA - Valutazione d'impatto sulla protezione dei dati (art. 35 GDPR)

La valutazione d'impatto sulla protezione dei dati personali è prevista quando un tipo di trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, e deve essere effettuata dal **Titolare** prima di procedere al trattamento.

Il **Titolare**, nello svolgimento della valutazione, deve consultare il **Responsabile** della protezione dei dati, di cui agli artt. 37 e ss del Regolamento (UE) 2016/679.

La valutazione è richiesta laddove venga effettuata una sorveglianza sistematica su larga scala di una zona accessibile al pubblico, ovvero qualora un trattamento *“possa presentare un rischio elevato”* ai sensi del GDPR (es: nell’ipotesi di utilizzo di un sistema di videosorveglianza per il controllo del traffico laddove si utilizzi un sistema intelligente di analisi delle immagini per l’individuazione dei veicoli e il riconoscimento automatico delle targhe).

La valutazione deve contenere almeno: **a)** una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l’interesse legittimo perseguito dal **Titolare** del trattamento; **b)** una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; **c)** una valutazione dei rischi per i diritti e le libertà degli interessati; **d)** le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati.

Se il trattamento è stato sottoposto a verifica preliminare da parte dell’Autorità Garante prima del maggio 2018 e prosegua con le stesse modalità oggetto di tale verifica, la valutazione non è necessaria, salvo che non siano emersi nuovi rischi.

La valutazione d’impatto non deve essere obbligatoriamente pubblicata, ma l’Amministrazione potrà valutare se pubblicarla integralmente o per estratto.

10.2 Consultazione preventiva (art. 36)

Qualora il Comune non sia in grado di individuare misure sufficienti a ridurre il rischio a livelli accettabili, e dunque qualora il rischio residuale continui a permanere elevato, si dovrà attuare la Consultazione preventiva con l’Autorità Garante prevista dall’art. 36 del Regolamento.

CAPO XI

COMUNICAZIONE E DIFFUSIONE DEI DATI

La comunicazione dei dati trattati dal Comune di Noragugume in conseguenza dell’azione delle videocamere dei sistemi di videosorveglianza complessivamente considerati, non potrà avvenire se non nei confronti dei soggetti ai quali lo stesso Comune deve comunicarli per effetto di obbligo di legge ovvero adempimento contrattuale oltre che per l’esercizio delle proprie pubbliche funzioni.

È in ogni caso fatta salva la comunicazione di dati richiesti, in conformità alla legge, da Forze di Polizia, dall’Autorità Giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

CAPO XII

CESSAZIONE DEL TRATTAMENTO DEI DATI PERSONALI

In caso di cessazione, per qualsiasi causa, di un trattamento, i dati personali sono distrutti, ceduti o conservati secondo quanto previsto dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e dal D.Lgs. 51/2018 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento perseguimento di reati o esecuzione di sanzioni penali.

CAPO XIII

TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Per tutto quanto attiene alla tutela amministrativa e giurisdizionale in tema di trattamento di dati personali mediante videosorveglianza si rinvia integralmente a quanto disposto dagli artt. 77 e ss, GDPR, nonché agli artt. 141 e ss. del Codice della privacy (D.lgs. 196/03 così come modificato dal D.lgs. 101/2018). 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 si rinvia agli artt. 37 e seguenti del D.Lgs. 51/2018.

CAPO XIV

MODIFICHE AL PRESENTE REGOLAMENTO

Il presente Regolamento dovrà essere aggiornato laddove intervengano modifiche normative in tema di trattamento di dati personali, nuovi provvedimenti del Garante della Privacy, ovvero significative modifiche nelle modalità e/o finalità dei trattamenti.

CAPO XV

DISPOSIZIONI FINALI

15.1 Entrata in vigore del presente Regolamento

Il presente Regolamento entra in vigore decorsi quindici giorni dalla data di pubblicazione all'Albo Pretorio online, fatti salvi gli eventuali tempi tecnici, che si rendessero necessari per l'organizzazione del servizio.

Eventuali e successive modifiche al presente Regolamento entreranno in vigore decorsi quindici giorni dalla data di pubblicazione all'Albo Pretorio online, da effettuarsi dopo che la relativa deliberazione di approvazione, ovvero determina dirigenziale, sia divenuta esecutiva.

Siffatto Regolamento, nonché le eventuali e successive modifiche, sono inseriti nella raccolta ufficiale dei Regolamenti Comunali.

15.2 Rinvio

Per quanto non previsto dal presente Regolamento, si rinvia alla normativa europea e nazionale in materia di trattamento e protezione dei dati personali nonché ai Provvedimenti dell'Autorità di controllo.

Il presente Regolamento sarà aggiornato a seguito delle modifiche della normativa e dei Provvedimenti di cui alla normativa vigente.

15.3 Norme abrogate

Con l'entrata in vigore del presente Regolamento si devono considerare abrogate le disposizioni regolamentari con esso contrastanti.

15.4 Pubblicità del presente Regolamento

Il presente Regolamento è pubblicato nel sito istituzionale del Comune di Noragugume.