



COMUNE DI NEONELI
PROVINCIA DI ORISTANO

**REGOLAMENTO SULLA
VIDEOSORVEGLIANZA**

Allegato alla deliberazione del C.C. n. 38 del 30.11.2022

Art. 1 – Premessa

Le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto a cui si riferiscono, costituiscono dati personali. La videosorveglianza dà luogo pertanto a trattamento di dati personali e incide sul diritto alla riservatezza delle persone fisiche eventualmente presenti nell'area sottoposta a ripresa.

Il presente regolamento garantisce che il trattamento dei dati personali, effettuato mediante sistemi di videosorveglianza gestiti ed impiegati dal Comune 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 - Normativa di riferimento e principi generali

Il presente regolamento disciplina il trattamento di dati personali realizzato mediante impianto di videosorveglianza attivato dal Comune di Neoneli (più avanti “Comune”) nel territorio comunale.

Per quanto non disciplinato dal presente regolamento, si rinvia alle seguenti normative:

- Decreto Ministero dell'Interno 05.08.2008;
- Legge n. 38/2009 recante “misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale nonché in tema di atti persecutori”;
- Regolamento UE Generale sulla Protezione dei Dati 2016/679 (di seguito RGPD) relativo “alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE”;
- Direttiva UE 2016/680 relativa “alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio”;
- DPR n. 15/2018 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 del 8.04.2010;
- Linee Guida 3/2019 sul trattamento di dati personali attraverso videosorveglianza del Comitato Europeo per la Protezione dei dati adottate il 29.01.2020.

Alla videosorveglianza si applicano i seguenti principi stabiliti dall'art. 5 del Regolamento UE Generale sulla Protezione dei Dati 2016/679 (più avanti “RGPD”):

Principio di liceità – Il trattamento di dati personali da parte di soggetti pubblici è lecito quando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Comune quale titolare del trattamento, ai sensi dell'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 dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Pertanto nei sistemi di videosorveglianza deve essere escluso ogni uso superfluo ed evitati eccessi e ridondanze. 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. È 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

Ai fini del presente regolamento si intende:

- per “dato personale”, qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- per “trattamento”, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- per “banca dati”, il complesso organizzato di dati personali, formatosi attraverso le apparecchiature di registrazione e ripresa video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nelle aree interessate dalle riprese;

- per “profilazione”, qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- per “pseudonimizzazione”, il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico, senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- per “titolare del trattamento”, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- per “autorizzato al trattamento”, la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del titolare o del designato al trattamento;
- per “titolare di posizione organizzativa designato allo svolgimento di specifici compiti e funzioni connessi al trattamento», la persona fisica designata che, sotto la responsabilità del titolare e nell'ambito della propria struttura organizzativa, svolge specifici compiti e funzioni connessi al trattamento dei 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 “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;
- per “comunicazione”, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- per “diffusione”, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- per “dato anonimo”, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Art. 4 – Finalità istituzionali del sistema di videosorveglianza

Le finalità perseguite dal Comune con l'attivazione di un sistema di videosorveglianza attengono allo svolgimento delle funzioni istituzionali proprie, in attuazione di quanto previsto dalle seguenti norme e circolari:

- D.Lgs. n. 267/2000 Testo unico delle leggi sull'ordinamento degli enti locali;
- D.P.R. n. 616/1977 Attuazione della delega di cui all'art. 1 della legge 22 luglio 1975, n. 382:

- D.Lgs. n. 112/1998 Conferimento di funzioni e compiti amministrativi dello Stato alle regioni ed agli enti locali, in attuazione del capo I della legge 15 marzo 1997, n. 59;
- Legge n. 65/1986 Ordinamento della Polizia Municipale;
- Legge n. 125/2008 Misure urgenti in materia di sicurezza pubblica;
- Legge n. 38/2009 sicurezza pubblica e di contrasto alla violenza sessuale;
- D. Ministero dell'Interno del 5.08.2008 in materia di incolumità pubblica e sicurezza urbana;
- Circolari del Ministero dell'Interno n. 558/A/421.2/70/456 del 8.02.2005, n. 558/A421.2/70/195860 del 6.08.2010 e n. 558/SICPART/421.2/70/224632 del 2.03.2012.

Nella predetta 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 è principalmente rivolto a garantire la sicurezza urbana, come definita dal D. Ministero dell'Interno del 5.08.2008.

La disponibilità tempestiva di immagini presso il Comune costituisce uno strumento di prevenzione e di razionalizzazione dell'azione della polizia locale sul territorio comunale, in stretto raccordo con le altre forze dell'ordine. L'archivio dei dati registrati costituisce, 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.

Il sistema di videosorveglianza del Comune 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; 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 del Comune e gli edifici pubblici e prevenire eventuali atti di vandalismo o danneggiamento;
- d) controllare le aree considerate a maggiore rischio per la sicurezza, l'incolumità e l'ordine pubblico;
- e) monitorare il traffico;
- f) attivare uno strumento operativo di protezione civile;
- g) acquisire elementi probatori in fattispecie di violazioni amministrative o penali;
- h) controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;
- i) monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti;
- j) verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti.

L'impianto di videosorveglianza non può essere utilizzato, in base all'art. 4 della legge 300/1970 (statuto dei lavoratori) per effettuare controlli sull'attività lavorativa dei dipendenti del Comune, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati. Gli impianti di

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

L'attività di videosorveglianza deve raccogliere solo i dati strettamente necessari al raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando quando non indispensabili immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza. La localizzazione delle telecamere e le modalità di ripresa sono sempre determinate in base ai richiamati principi.

La possibilità di avere in tempo reale dati e immagini costituisce uno strumento di prevenzione e di razionalizzazione dei compiti che la polizia locale svolge quotidianamente nell'ambito delle proprie competenze istituzionali; attraverso tali strumenti si perseguono finalità di tutela della popolazione e del patrimonio comunale, garantendo un elevato grado di sicurezza nei luoghi di maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, artistico e culturale, negli edifici pubblici, nel centro storico, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare.

L'uso dei dati personali nell'ambito definito dal presente regolamento non necessita del consenso degli interessati, in quanto è 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

Nell'ufficio di polizia locale del Municipio saranno posizionati i monitor per la visione in diretta delle immagini riprese dalle telecamere e le apparecchiature per la relativa registrazione.

L'impianto di videosorveglianza che sarà installato nel Comune è suscettibile di future implementazioni e adeguamenti alle esigenze tecnologiche e/o normative.

Le telecamere consentiranno riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario.

Gli impianti da installare nella fase iniziale sono i seguenti: n. 4 telecamere (municipio, scuola primaria, varco 1, varco 2) collegate alla centrale operativa del Comune, più una workstation.

La documentazione concernente le caratteristiche tecnico-funzionali del sistema e gli strumenti utilizzati per la videosorveglianza sarà conservata presso l'ufficio di polizia locale (vedere anche il seguente link: <https://www.unionecomunibarigadu.it/ente/atti/evidenza/3570>), tenuta aggiornata dal dipendente incaricato in modo da essere disponibile in caso di ispezioni o di controlli da parte delle autorità competenti.

Il Comune quale titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità previste.

I segnali video delle unità di ripresa saranno raccolti da una stazione di monitoraggio e controllo ubicata in un apposito locale tecnico adibito al solo ed esclusivo utilizzo del sistema di videosorveglianza. In questa sede le immagini possono essere visualizzate su monitor e registrate su un supporto magnetico o allo stato solido, in dipendenza delle soluzioni tecniche prescelte. L'impiego del sistema di videoregistrazione è necessario per ricostruire l'evento secondo le finalità previste dal presente regolamento.

Le immagini videoregistrate sono conservate, per un tempo non superiore a 7 (sette) giorni successivi alla rilevazione, presso il datacenter dove sono posizionati i dispositivi di memorizzazione e immagazzinamento delle riprese.

Il predetto termine di conservazione è ritenuto proporzionato, tenuto conto degli atti di vandalismo, furti e altri incidenti accaduti nel territorio comunale nel corso degli ultimi anni, a gestire ogni

situazione rientrante nella finalità sopra indicata, considerate le specifiche esigenze di sicurezza perseguite. Le immagini riprese in tempo reale sovrascriveranno quelle registrate, garantendo il rispetto del termine massimo di conservazione.

Il sistema di registrazione posizionato nei locali del Municipio sarà attivo e potrà essere tele-gestito dalla stanza di controllo con orario continuato, 24 ore su 24 e 365 giorni l'anno, dal responsabile del trattamento dei dati, autorizzato alla manutenzione e gestione del sistema di videosorveglianza.

Sarà cura del responsabile del trattamento dei dati, in caso di eventi di natura criminosa e/o su richiesta, estrapolare le immagini video e metterle a disposizione delle forze dell'ordine che ne facciano formale richiesta al Comune, con l'osservanza delle norme del presente regolamento.

Il collegamento all'impianto di videosorveglianza può essere esteso alle forze di polizia che ne facciano formale richiesta al Comune, con l'osservanza delle norme del presente regolamento.

In relazione ai principi di pertinenza e di non eccedenza, 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

Gli interessati devono essere sempre informati che stanno per accedere ad una zona videosorvegliata.

A tal fine il Comune deve rendere disponibili informazioni di primo livello, mediante utilizzo di un segnale di avvertimento indicante le informazioni più importanti, quali l'identità del titolare del trattamento, i dettagli della finalità perseguita, i diritti dell'interessato e le informazioni sui maggiori impatti del trattamento. Ciò può includere, ad esempio, gli interessi legittimi perseguiti dal titolare del trattamento (o da una terza parte) e i dettagli di contatto del titolare della protezione dei dati.

L'informativa di primo livello deve comprendere almeno l'indicazione dell'eventuale trasmissione di dati a terzi ed il periodo di conservazione dei dati acquisiti mediante l'impianto di videosorveglianza.

Si allega al presente regolamento lo schema di informativa di primo livello, risultante dalle Linee Guida 3/2019 del Comitato Europeo sul trattamento dei dati personali del 10.07.2019 approvato il 29.01.2020, tenuto conto del Provvedimento del Garante per la Protezione dei dati Personali del 08.04.2010.

Il Servizio Tecnico del Comune provvederà ad affiggere la segnaletica informativa permanente in corrispondenza di ciascun varco (pedonale e carrabile) di accesso all'area sulla quale insistono gli immobili oggetto di videosorveglianza. Su detta segnaletica è riportata l'informativa sopra illustrata.

La segnaletica deve essere collocata prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno.

In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, devono essere installati più cartelli informativi.

Le informazioni di secondo livello devono essere rese disponibili in un luogo facilmente accessibile all'interessato, mediante pannello informativo analogico o digitale. Il segnale di avvertimento di primo livello deve operare un rinvio alle informazioni di secondo livello. Le informazioni del primo livello possono anche fare riferimento a una fonte digitale (ad esempio QR-code o indirizzo di un sito Web) delle informazioni di secondo livello.

In ogni caso, deve essere possibile accedere alle informazioni di secondo livello senza entrare nell'area rilevata. Le informazioni devono contenere tutte le informazioni obbligatorie ai sensi dell'art. 13 del GDPR.

Il Comune deve informare gli utenti dei servizi dell'avvio del trattamento dei dati personali con l'attivazione dell'impianto di videosorveglianza, dell'eventuale incremento dimensionale dell'impianto e dell'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, con un anticipo di giorni dieci, mediante affissione di appositi manifesti informativi o altro sistema di comunicazione diretta.

Art. 7 - Valutazione di impatto sulla protezione dei dati

Ai sensi dell'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 e qualora presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il Comune procederà ad una valutazione di impatto sulla protezione dei dati personali.

Il Responsabile del Servizio incaricato in base all'art. 9, ai sensi dell'art. 35, paragrafi 4 e 5, RGPD, verificherà la pubblicazione da parte dell'Autorità Garante per la protezione dei dati personali dell'elenco delle tipologie di trattamenti soggetti alla valutazione di impatto e la pubblicazione dell'elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione di impatto.

Art. 8 - Titolare del trattamento

Il titolare del trattamento dei dati è il Comune.

Spetta agli organi politici e gestionali del Comune, secondo le rispettive competenze, 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.

Art. 9 – Titolare di posizione organizzativa incaricato di specifici compiti e funzioni connessi al trattamento dei dati

Il Responsabile del Servizio Tecnico del Comune sarà incaricato dal Sindaco con decreto dello svolgimento di specifici compiti e funzioni di vigilanza e controllo connessi al trattamento dei dati personali rilevati attraverso il sistema di videosorveglianza.

Il Responsabile del Servizio incaricato deve conformare la propria azione al pieno rispetto di quanto prescritto dalle disposizioni normative in materia e dal presente regolamento.

Il Responsabile del Servizio incaricato procede al trattamento dei dati attenendosi al presente regolamento e alle istruzioni date dal Sindaco il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.

I compiti e le funzioni specifiche attribuite al Responsabile del Servizio incaricato sono analiticamente disciplinati nel decreto di nomina del Sindaco e sono i seguenti:

- fornire al Sindaco l'elenco nominativo dei dipendenti che, nell'esercizio dei compiti d'istituto, hanno accesso ai dati oggetto di rilevazione, autorizzati dallo stesso Responsabile di Servizio al trattamento dei dati;
- predisporre l'informativa minima agli interessati ai sensi dell'art. 6, in conformità alle specifiche tecnico-operative del sistema di videosorveglianza;
- individuare con specifico provvedimento i dipendenti autorizzati al trattamento dei dati personali acquisiti con l'impianto di videosorveglianza;

- dare agli autorizzati al trattamento istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati, ai sensi dell’art. 29, RGPD; le persone autorizzate devono essere istruite e formate a cura del Responsabile del Servizio incaricato circa la tutela del diritto alla riservatezza, nonché le misure tecniche e organizzative da osservare per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati;
- controllare che il trattamento dei dati effettuato con il sistema di videosorveglianza sia realizzato nel rispetto dei principi di cui all’art. 5 del RGPD e, in particolare, assicurare che i dati personali siano trattati in modo lecito, corretto e trasparente, siano acquisiti e trattati esclusivamente per le finalità determinate, esplicite e legittime connesse all’esercizio del sistema di videosorveglianza;
- assicurare che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- tenuto conto dello stato dell’arte, della natura, dell’oggetto, del contesto, delle finalità del trattamento e del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, adottare tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell’art. 32 del RGPD;
- assistere il Sindaco al fine di consentire allo stesso di rispondere alle richieste per l’esercizio dei diritti dell’interessato di cui al Capo III del RGPD;
- assistere il Sindaco nel garantire il rispetto degli obblighi di sicurezza di cui all’art. 32 RGPD e coadiuvarlo nella concreta adozione di misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; qualora a ciò non possa provvedere immediatamente con i mezzi assegnati, è responsabile della tempestiva formulazione della proposta alla Giunta Comunale di adozione delle misure necessarie;
- garantire l’adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l’accesso agli stessi in caso di incidente fisico o tecnico; qualora a ciò non possa provvedere immediatamente con i mezzi assegnati, formalizzare tempestivamente la proposta alla Giunta Comunale di adozione delle misure necessarie;
- assistere il Sindaco nelle eventuali procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all’interessato ai sensi degli artt. 33 e 34 del RGPD;
- assistere il Sindaco nell’effettuazione della valutazione di impatto sulla protezione dei dati, ai sensi dell’art. 35 del RGPD e dell’art. 7 del presente regolamento e nella successiva eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità all’art. 36 del RGPD;
- provvedere, ai sensi dell’art. 30, paragrafo 1, del RGPD, all’istituzione e aggiornamento del registro delle attività di trattamento, anche in formato elettronico;
- fornire al Responsabile per la Protezione dei Dati ogni elemento, dato e informazione necessari alla regolare formazione, tenuta e all’aggiornamento del registro delle attività dei trattamenti di cui all’art. 30, paragrafo 1, RGPD;
- garantire che il Responsabile della Protezione dei Dati nominato dal Sindaco sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e si impegna ad assicurargli l’affiancamento necessario per l’esecuzione dei suoi compiti;
- custodire e controllare i dati personali di competenza, affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

- assicurare che i dipendenti autorizzati al trattamento dei dati personali si attengano al perseguimento delle finalità per le quali il trattamento è consentito e garantire che siano compiute solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali;
- garantire la tempestiva emanazione di direttive ed ordini di servizio scritti ai dipendenti individuati quali incaricati del trattamento realizzato con l'impianto di videosorveglianza del Comune, previo consulto con il Responsabile della Protezione dei Dati, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;
- vigilare sul rispetto da parte dei dipendenti autorizzati al trattamento dei dati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.

Per l'espletamento dei compiti predetti, il Responsabile di Servizio incaricato si avvale di responsabili del trattamento che, incaricati della gestione/assistenza del sistema di videosorveglianza nell'ambito di servizi, lavori, forniture, consulenze che comportino un trattamento di dati per conto del Comune, presentino garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate che assicurino la tutela dei diritti dell'interessato. In questi casi, il designato al trattamento procederà a disciplinare i trattamenti da parte del responsabile nell'ambito del contratto di appalto o di altro atto giuridico che vincoli il responsabile del trattamento al Comune quale titolare del trattamento, ai sensi dell'art. 28 RGPD.

Compete al Responsabile del Servizio incaricato l'approvazione dei provvedimenti attuativi, nonché la definizione di ogni ulteriore e specifica disposizione ritenuta utile, in coerenza con gli indirizzi stabiliti dal presente regolamento.

Art. 10 – Dipendenti autorizzati al trattamento dei dati

I dipendenti autorizzati al trattamento dei dati, all'utilizzazione dell'impianto di videosorveglianza e, nei casi in cui sia indispensabile per gli scopi perseguiti, alla visione delle registrazioni, sono individuate con atto del Responsabile del Servizio incaricato, ai sensi dell'art. 2-quaterdecies, comma 2, del D.Lgs. 196/2003.

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

Prima dell'utilizzo degli impianti, le persone autorizzate devono essere adeguatamente formate circa il corretto uso del sistema, circa la normativa di riferimento ed il presente regolamento e dovranno conformare la propria condotta al pieno rispetto del medesimo.

I dipendenti autorizzati procedono al trattamento attenendosi al presente regolamento e alle istruzioni del Responsabile del Servizio incaricato il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.

I dipendenti autorizzati devono:

- utilizzare sempre per l'accesso alle banche dati informatiche 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 Responsabile del Servizio incaricato al 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 dal Comune;
- fornire al Responsabile del Servizio incaricato ed al Responsabile della Protezione dei Dati, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire un'efficace attività di controllo.

Tra i dipendenti autorizzati saranno individuate nell'atto di nomina le persone cui è affidata la custodia e la conservazione delle chiavi di accesso alla sala operativa e agli armadi per la conservazione dei supporti magnetici.

Le persone autorizzate al trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi al presente regolamento e alle istruzioni del Responsabile del Servizio incaricato.

L'utilizzo degli apparecchi di ripresa da parte delle persone autorizzate al trattamento deve essere conforme ai limiti stabiliti dal presente regolamento.

Art. 11 - Modalità di raccolta e di trattamento dei dati

L'installazione delle telecamere di videosorveglianza è possibile solo nei luoghi pubblici (strade, piazze, immobili), in base all'elenco dei siti di ripresa predisposto dall'Amministrazione Comunale.

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

Le telecamere consentono riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario.

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

I dati personali oggetto di trattamento sono:

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

La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata a 7 (sette) giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, in base alle richiamate disposizioni normative, il termine massimo di durata della conservazione dei dati è limitato a 7 (sette) giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante il sistema di videosorveglianza, fatte salve specifiche esigenze di ulteriore conservazione.

In ragione di necessità investigative e su richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria il Comune quale titolare del trattamento potrà disporre la conservazione delle immagini per un periodo di tempo superiore a 7 (sette) giorni, previa richiesta al Garante per la protezione dei dati personali che, a seguito di verifica preliminare, potrà rilasciare parere favorevole.

Il sistema di videoregistrazione impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati, allo scadere del termine di 7 (sette) giorni, come previsto dal Provvedimento del Garante della Privacy del 08.04.2010, in attuazione della finalità di sicurezza urbana di cui all'art. 2 del presente regolamento.

In caso di cessazione del trattamento, i dati personali devono essere integralmente distrutti.

Art. 12 - Sicurezza dei dati

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

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

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

Ai sensi dell'art. 32, paragrafo 2, RGPD, nel valutare l'adeguato livello di sicurezza, l'Amministrazione Comunale 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 dal Comune.

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

- a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi privilegi di visibilità e di trattamento delle immagini. Tenendo conto dello stato dell'arte ed in base alle caratteristiche dei sistemi utilizzati, i soggetti autorizzati al trattamento dovranno essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti a ciascuno, unicamente le operazioni di competenza;
- b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, dovrà essere attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime immagini operazioni di cancellazione o di duplicazione;
- c) per quanto riguarda il periodo di conservazione delle immagini indicato all'art. 10, dovranno essere predisposte misure tecniche per la cancellazione, in forma automatica, delle registrazioni, allo scadere del termine previsto;

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

Come indicato all'art. 9, il Sindaco quale legale rappresentante del Comune titolare del trattamento attribuisce per iscritto ad un Responsabile di Servizio specifici compiti e funzioni connessi al trattamento di dati personali.

Come indicato all'art. 10, il Responsabile del Servizio incaricato individua per iscritto i dipendenti autorizzati al trattamento ed abilitati ad accedere ai locali dove sono situate le postazioni di controllo, ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini.

Art. 13 – Accesso ai dati

L'accesso ai dati registrati al fine del loro riesame, nell'arco temporale previsto per la conservazione, è consentito solo in caso di effettiva necessità, per le finalità istituzionali di cui all'art. 4.

L'accesso alle immagini videoregistrate è consentito esclusivamente:

- al Sindaco e ai dipendenti autorizzati al trattamento;
- alle Forze di Polizia, sulla base di formale richiesta del rispettivo comando di appartenenza acquisita al protocollo del Comune e per finalità di indagine dell'Autorità Giudiziaria, sulla base di formale richiesta del Pubblico Ministero acquisita al protocollo del Comune;
- alla società fornitrice dell'impianto o al soggetto incaricato della manutenzione, nei limiti strettamente necessari alle specifiche esigenze di funzionamento e manutenzione dell'impianto o se e quando necessario all'amministratore del sistema informatico comunale, preventivamente individuato quale incaricato del trattamento dei dati;
- all'interessato del trattamento, in quanto oggetto delle riprese, che abbia presentato richiesta di accesso alle immagini, previo accoglimento della stessa secondo il procedimento descritto al successivo art. 14; l'accesso da parte dell'interessato deve essere limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, deve essere utilizzata, in conformità alle istruzioni impartite dal Responsabile del Servizio incaricato, una schermatura/sfocatura del video o altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi di altre persone fisiche eventualmente presenti;
- ai soggetti legittimati all'accesso ai sensi degli artt. 22 e seguenti della L. 241/1990 e nei casi in cui, ai sensi dell'art. 24, comma 7, L. 241/1990, l'accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente; l'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente

presenti, non strettamente indispensabili per la difesa degli interessi giuridici del soggetto richiedente.

Art. 14 - Diritti dell'interessato

In relazione al trattamento di dati personali che lo riguardano, l'interessato, ai sensi degli artt. 15 e seguenti RGPD, su presentazione di apposita richiesta, ha diritto:

- di ottenere dal Comune 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 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;
- 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.

La richiesta dell'interessato per l'esercizio dei diritti deve essere presentata al Titolare del trattamento dati del Comune, ai sensi dell'art. 38, paragrafo 4, RGPD, i cui dati di contatto devono essere resi disponibili sulla home page del sito istituzionale del Comune alla Sezione Amministrazione Trasparente.

Nella richiesta di accesso alle immagini l'interessato dovrà 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.

Il Responsabile della Protezione dei Dati del Comune o il Responsabile del Servizio incaricato accerta l'effettiva esistenza delle immagini e ne dà comunicazione al richiedente; nel caso di accertamento positivo fissa il giorno, l'ora ed il luogo in cui l'interessato può prendere visione delle immagini che lo riguardano.

Se, ai sensi dell'art. 15, paragrafo 3, RGPD, l'interessato chiedi di avere copia dei dati personali oggetto di trattamento, il Responsabile del procedimento procede 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, ai sensi dell'art. 15, paragrafo 4, RGPD.

I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire per iscritto procura a persone fisiche, enti, associazioni od organismi e farsi assistere da persona di fiducia.

Nel caso di esito negativo della richiesta, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Art. 15 – Tutela dell'interessato - diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali

Qualora l'interessato ritenga che i diritti di cui gode sulla base della normativa in materia di protezione dei dati personali siano stati violati, può proporre reclamo al Garante o ricorso dinanzi all'autorità giudiziaria, ai sensi dell'art. 140-bis del D.Lgs. 196/2003.

Per quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia a quanto disposto dagli artt. 77 e seguenti RGPD.

Il reclamo al Garante, ai sensi dell'art. 77 del RGPD, non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria (art. 140-bis, comma 2, del D.Lgs. 196/2003).

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

Le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli artt. 78 e 79 del regolamento, nonché il diritto al risarcimento del danno, sono attribuite all'autorità giudiziaria ordinaria (art. 152 del D.Lgs. 196/2003).

Chiunque ritenga di aver subito un danno materiale o immateriale per effetto del trattamento di dati personali ha il diritto di ottenere il risarcimento del danno, ai sensi dell'art. 82 RGPD.

Art. 16 - Pubblicità del regolamento

Il presente regolamento sarà pubblicato sul sito internet del Comune www.comune.neoneli.or.it per 15 giorni all'albo pretorio informatico e a permanenza nella sezione Amministrazione Trasparente – sottosezione Disposizioni generali – sottosezione Atti generali.

Art. 17 – Entrata in vigore

Il presente regolamento entrerà in vigore alla data di esecutività della deliberazione di approvazione ed abroga ogni regolamento precedente che disciplina la materia.



VIDEOSORVEGLIANZA



Ulteriori informazioni sono
disponibili sul sito internet del
Comune
www.comune.neoneli.or.it

**Dati identificativi del Titolare del trattamento e del
rappresentante del Titolare del trattamento:**

Comune di Neoneli – Sindaco Salvatore Cau

Dati di contatto del Responsabile della Protezione dei Dati:

SIPAL Srl - Cagliari - Mail: dpo@sipal.sardegna.it

I dati acquisiti saranno trasmessi a:

**I dati acquisiti saranno conservati su supporti magnetici per 7 giorni e
al termine cancellati e non più recuperabili**

Finalità e base giuridica del trattamento: per motivi di tutela della
sicurezza pubblica; art. 6, paragrafo 1, lett. e) Regolamento UE 2016/679

Diritti degli interessati: in quanto soggetto interessato hai diversi
diritti nei confronti del Comune, in particolare il diritto di richiedere
l'accesso o la cancellazione dei tuoi dati personali.

Per i dettagli su questa videosorveglianza, inclusi i tuoi diritti,
consulta le informazioni complete fornite dal Comune attraverso le
opzioni indicate a sinistra.