



COMUNE DI NEGRAR DI VALPOLICELLA
Provincia di Verona

REGOLAMENTO COMUNALE SULLA VIDEOSORVEGLIANZA

DELIBERAZIONE DEL CONSIGLIO COMUNALE N. 10 DEL 10.02.2020

Indice

CAPO I - PRINCIPI GENERALI

Art. 1 - Premessa.....	2
Art. 2 - Norme di riferimento e principi generali.....	2
Art. 3 - Definizioni.....	3
Art. 4 - Finalità istituzionali dei sistemi di videosorveglianza	4

CAPO II - MISURE ORGANIZZATIVE PER IL TRATTAMENTO DEI DATI..... 5

Art. 5 - Titolare del trattamento	5
Art. 6 - Struttura organizzativa e autorizzati al trattamento.....	5
Art. 7 - Contitolari.....	6
Art. 8 - Terzi autorizzati all'accesso	6
Art. 9 - Affidamenti esterni e responsabili del trattamento.....	6

CAPO III - MISURE TECNICHE PER IL TRATTAMENTO DEI DATI E MISURE DI SICUREZZA..... 7

Art. 10 - Trattamenti e conservazione dei dati.....	7
Art. 11 - Specificità per Body Cam, Dash Cam e telecamere su droni.....	8
Art. 12 - Sicurezza dei dati.....	9
Art. 13 - Cessazione del trattamento dei dati	9
Art. 14 - Valutazione di Impatto sulla protezione dei dati.....	10

CAPO IV - DIRITTI E LIMITI NEL TRATTAMENTO DEI DATI, INFORMATIVA E VALUTAZIONE DI IMPATTO 10

Art. 15 - Diritti dell'interessato.....	10
Art. 16 - Informativa	11
Art. 17 - Limiti alla utilizzabilità di dati personali	11
Art. 18 - Danni cagionati per effetto del trattamento di dati personali	12
Art. 19 - Comunicazione.....	12

CAPO V - TUTELA AMMINISTRATIVA E GIURISDIZIONALE: NORME FINALI..... 12

Art. 20 - Tutela.....	12
Art. 21 - Provvedimenti attuativi	12
Art. 22 - Norma di rinvio	12
Art. 23 - Pubblicità del Regolamento.....	13
Art. 24 - Entrata in vigore	13

CAPO I - PRINCIPI GENERALI

Art. 1 - Premessa

1. Il presente Regolamento disciplina le modalità di raccolta, trattamento e conservazione dei dati personali mediante sistemi di videosorveglianza gestiti, nell'ambito del proprio territorio, dal Comune di Negrar di Valpolicella.
2. Costituisce videosorveglianza quel complesso di strumenti finalizzati alla vigilanza in remoto, cioè che si realizza a distanza mediante dispositivi per le riprese video collegati a un centro di controllo e coordinamento direttamente gestito da personale della Polizia Locale di Negrar di Valpolicella. Le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto a cui si riferiscono, costituiscono dati personali. In tali casi la videosorveglianza incide sul diritto delle persone alla propria riservatezza.
3. Il presente Regolamento garantisce che il trattamento dei dati personali, effettuato mediante sistemi di videosorveglianza gestiti ed impiegati dal Comune nel proprio territorio, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. Garantisce altresì i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento.

Art. 2 - Norme di riferimento e principi generali

1. Il presente regolamento disciplina il trattamento di dati personali, realizzato mediante l'impianto di videosorveglianza cittadina, attivato nel territorio comunale.
2. Per tutto quanto non dettagliatamente disciplinato dal presente Regolamento, si rinvia a quanto disposto da:
 - a. 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";
 - b. 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" che abroga la decisione quadro 2008/977/GAI del Consiglio;
 - c. Decreto Legislativo n. 51 del 18 maggio 2018;
 - d. Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza del 8 aprile 2010 (G.U. n. 99 del 29/04/2010);
 - e. Decreto Ministero dell'Interno 05/08/2008 (G.U. n. 186 del 09.08.2008);
 - f. Legge n. 38/2009 recante "misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale nonché in tema di atti persecutori";
 - g. Decreto Legge 11/2009, convertito nella legge 23 aprile 2009.;
 - h. Article 29 Data Protection Working Party, "Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones":
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf.
 - i. Regolamento di esecuzione (UE) 2019/947 della commissione del 24 maggio 2019 relativo a norme e procedure per l'esercizio di aeromobili senza equipaggio
3. La Videosorveglianza in ambito Comunale si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5 del RGPD e, in particolare:

- a. *Principio di liceità*: il trattamento di dati personali da parte di soggetti pubblici è lecito allorché è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento in ossequio al disposto di cui all'art. 6, Paragrafo 1, lett. e), RGPD.
- b. *Principio di necessità*: il sistema di videosorveglianza è configurato per ridurre al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di videosorveglianza. Inoltre, il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati

- c. *Principio di proporzionalità*: la raccolta e l'uso delle immagini devono essere proporzionali agli scopi perseguiti. 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. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano 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.
- d. *Principio di finalità*: gli scopi perseguiti devono essere determinati, espliciti e legittimi (Art. 5, Paragrafo 1, lett. b) del RGPD), e successivamente trattati in modo che non sia incompatibile con tali finalità. Pertanto è consentita la videosorveglianza come misura complementare volta a migliorare e garantire la **sicurezza urbana**, che il DM Interno 05/08/2008 definisce come il "bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale."

Art. 3 - Definizioni

1. Ai fini del presente Regolamento si intende:

- a. 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;
- b. 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;
- c. per "*banca di dati*", il complesso di dati personali, formatosi presso apparecchiature di registrazione e ripresa video, che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto;

- d. per “*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; nella fattispecie è il Comune di Negrar di Valpolicella di Valpolicella;
- e. per “*responsabile*”, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- f. per “*incaricato*” o “*autorizzato*”, la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del titolare o del responsabile del trattamento;
- g. per “*interessato*”, la persona fisica cui si riferiscono i dati personali;
- h. 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;
- i. per “*violazione dei dati personali*”, la violazione di sicurezza che comporta accidentalmente o in modo illecito l'accesso, la distruzione, la perdita, la modifica, la divulgazione non autorizzata dei dati personali trasmessi, conservati o comunque trattati;
- j. per “*comunicazione*”, il dare conoscenza dei dati personali a soggetti determinati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- e. per “*diffusione*”, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- f. per “*dato anonimo*”, il dato che in origine, per le modalità di inquadratura o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- g. per “*blocco*”, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
- a. per *sicurezza urbana* si intendere la tutela della sicurezza pubblica, in quanto attività di prevenzione e repressione dei reati, con esclusione delle funzioni di polizia amministrativa (art. 6 del DL 23 febbraio 2009, n. 11).

Art. 4 - Finalità istituzionali dei sistemi di videosorveglianza

1. Le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza sono conformi alle funzioni istituzionali attribuite al Comune di Negrar di Valpolicella dalle leggi, di cui all'articolo 2, e dai Regolamenti comunali vigenti.
2. Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato per le seguenti finalità:
 - a. presidiare e tutelare il patrimonio comunale, le aree adiacenti ad uffici od immobili comunali, oltre a particolari e specifici siti comunali;
 - b. tutelare la sicurezza urbana e la pubblica sicurezza;
 - c. tutelare e monitorare la sicurezza stradale, controllando la circolazione lungo le strade del territorio comunale;
 - d. tutelare l'ambiente;
 - e. tutelare la sicurezza degli agenti di polizia locale.
3. Il sistema di videosorveglianza comporta il trattamento di dati personali rilevati mediante le riprese video che, in relazione ai luoghi di installazione delle telecamere, interessano i soggetti ed i mezzi di trasporto che transitano nell'area interessata.
4. Il Comune promuove ed attua, per la parte di competenza, politiche di controllo del territorio integrate con organi istituzionalmente preposti alla tutela della sicurezza e dell'ordine pubblica. A tal fine il Comune, previa intesa o su richiesta delle autorità di pubblica sicurezza o degli organi di polizia, può disporre l'utilizzo degli impianti comunali di videosorveglianza anche ai

fini di prevenzione e repressione di atti delittuosi. I dati così raccolti vengono utilizzati esclusivamente dalle autorità ed organi anzidetti.

5. Conformemente a quanto previsto dall'articolo 4 della Legge 20 maggio 1970, n. 300 è vietato, e pertanto escluso, l'uso degli impianti di videosorveglianza per effettuare controlli a distanza sull'attività lavorativa dei dipendenti dell'amministrazione, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

CAPO II - MISURE ORGANIZZATIVE PER IL TRATTAMENTO DEI DATI

Art. 5 - Titolare del trattamento

1. Titolare del trattamento è il comune di Negrar di Valpolicella, al quale compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza da adottare. I trattamenti sono descritti al successivo Art. 10.
2. Il Titolare deve garantire il rispetto degli obblighi di sicurezza di cui all'art. 32 del RGPD, mettendo in atto misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

Art. 6 - Struttura organizzativa e autorizzati al trattamento

1. Compete al Sindaco designare per iscritto gli autorizzati al trattamento dei dati mediante il sistema di videosorveglianza, all'utilizzo degli impianti e, nei casi in cui risulta indispensabile per gli scopi perseguiti, alla visione delle registrazioni.
2. Il Sindaco delega il coordinamento operativo e la sorveglianza sull'utilizzo dell'impianto al Comandante della Polizia Locale in servizio, o altro addetto alla Polizia Locale, tramite nomina da effettuare con opportuno atto.
3. Il compito affidato al Comandante deve essere svolto nel rispetto della normativa vigente in tema di trattamento dei dati personali, ivi incluso il profilo della sicurezza, ed delle disposizioni del presente Regolamento.
4. Il Comandante deve:
 - a. procedere al trattamento attenendosi alle presenti istruzioni;
 - b. vigilare, anche tramite verifiche periodiche, sulla puntuale osservanza delle disposizioni previste dalla normativa vigente e delle presenti istruzioni da parte del personale autorizzato;
 - c. vigilare, anche tramite verifiche periodiche, sull'operato da parte di eventuali responsabili (aziende esterne);
 - a. custodire le chiavi per l'accesso ai locali della della Polizia Locale, nonché le proprie parole chiave per l'accesso ai sistemi;
 - b. sovrintendere all'accesso per la manutenzione e riparazione degli impianti.
5. Il Comandante individua e propone gli autorizzati della gestione dell'impianto, in numero ritenuto sufficiente a garantire la corretta gestione del servizio di videosorveglianza.
6. Tali persone sono individuate nell'ambito degli appartenenti al Comando di Polizia Locale, tra coloro che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati, e sono dotate della qualifica di agenti di Pubblica Sicurezza.

Con l'atto di nomina, ai singoli autorizzati sono affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi.

7. In ogni caso, prima dell'utilizzo degli impianti, essi saranno istruiti al corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento.
8. Ciascun autorizzato deve utilizzare le proprie credenziali, composte da nome utente e password; la password è nota a lui solo.
9. La visione delle immagini registrate è consentita, oltre agli autorizzati, anche a chi esercita funzioni di polizia giudiziaria, ed al personale esterno addetto alla manutenzione ed alle riparazioni, quest'ultimo sempre previa autorizzazione del Titolare.

Art. 7 - Contitolari

1. Il sistema di riconoscimento targhe viene esercito in contitolarità con il comune di S. Pietro in Cariano, che lo ospita fisicamente. Il comune di Negrar di Valpolicella, nel cui territorio vengono rilevati i dati, assume il ruolo di contitolare, ed autorizza il trattamento con la relativa convenzione per la realizzazione e gestione dell'impianto.

Art. 8 - Terzi autorizzati all'accesso

1. Sono autorizzati all'accesso, oltre agli addetti di Polizia Locale, tutti coloro che hanno la qualifica di Ufficiali ed Agenti di Polizia Giudiziaria ai sensi dell'art. 55 del Codice di Procedura Penale.
2. Nel caso in cui i Corpi e gli organi di Polizia, nello svolgimento di loro indagini, necessitino di avere informazioni ad esse collegate, che possono essere contenute nelle riprese effettuate, possono inoltrare richiesta scritta e motivata indirizzata al Titolare del trattamento dei dati.
3. L'accesso diretto al sistema dovrà essere regolato da apposita convenzione. Detta convenzione dovrà rispettare le norme tecniche descritte ai successivi Artt. 10 e 12.

Art. 9 - Affidamenti esterni e responsabili del trattamento

1. Qualora lo ritenesse opportuno o necessario (per esempio per eseguire la manutenzione tecnica) il titolare può delegare aziende od enti esterni come Responsabili del trattamento.
2. Le competenze proprie del Responsabile del trattamento sono analiticamente disciplinate nel contratto ovvero nell'atto giuridico avente forma scritta, con il quale il Titolare provvede alla sua designazione.
3. Il Responsabile del trattamento è tenuto a conformare la propria azione al pieno rispetto di quanto prescritto dalle vigenti disposizioni normative in materia e dal presente Regolamento.
4. Il Responsabile procede al trattamento dei dati attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.
5. Il Responsabile del trattamento individua e nomina con propri atti gli Incaricati del trattamento impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in conformità alle previsioni di cui all'art. 18 Dlgs 51/2018; detti incaricati sono opportunamente istruiti e formati da parte del Responsabile del trattamento per:
 - a. eseguire solamente le operazioni strettamente necessarie al perseguimento delle finalità descritte nel presente regolamento,
 - b. attenersi alle le misure tecniche e organizzative necessarie a ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati.
6. Il Responsabile del trattamento vigila sul rispetto da parte degli incaricati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.
7. Il Responsabile del trattamento assiste il Titolare al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del RGPD;

8. Il Responsabile del trattamento assiste il Titolare nel garantire il rispetto degli obblighi di sicurezza di cui all'art. 25 del Dlgs 51/2018, mettendo in atto misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti dell'Ente;
9. il Responsabile del trattamento assicura l'adozione di procedure volte a testare, verificare e valutare costantemente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento.
10. il Responsabile del trattamento assiste il Titolare ed il Responsabile della Protezione dei Dati (RPD) 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 art. 33 e 34 del RGPD;
11. il Responsabile del trattamento assiste il Titolare nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 23 del Dlgs 51/2018;
12. il Responsabile del trattamento affianca il Titolare, in conformità alle disposizioni di cui all'art. 30, paragrafo 1, del RGPD, nell'istituzione e aggiornamento del Registro delle attività di trattamento, tenuto in forma scritta, anche in formato elettronico;
13. il Responsabile del trattamento garantisce che il Responsabile della Protezione dei Dati (noto anche con la sigla DPO), designato dal Titolare del trattamento, sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e si impegna ad assicurargli l'affiancamento necessario per l'esecuzione dei suoi compiti;
14. il Responsabile del trattamento mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa e per consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto incaricato;
15. Il Responsabile del trattamento è responsabile della custodia e del controllo dei dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
16. Il Responsabile del trattamento può ricorrere a ulteriori Responsabili solo previa autorizzazione del Titolare.

CAPO III -

MISURE TECNICHE PER IL TRATTAMENTO DEI DATI E MISURE DI SICUREZZA

Art. 10 - Trattamenti e conservazione dei dati

1. I sistemi di raccolta dei dati oggetto di trattamento utilizzati dal comune sono:
 - a. videosorveglianza tramite telecamere e fotocamere;
 - b. videosorveglianza con riconoscimento targhe;
 - c. telecamere a bordo di servizio (dash cam);
 - d. telecamere indossabili (body cam) utilizzate dalla polizia municipale durante le operazioni;
 - e. telecamere montate a bordo di droni radiocomandati.
2. La *videosorveglianza tramite telecamere* viene effettuata attraverso riprese video da sistemi di telecamere a circuito chiuso installate in corrispondenza delle principali strade, piazze, luoghi pubblici ed immobili di proprietà comunale, ubicati nel territorio comunale.
3. Le telecamere di cui al precedente comma consentono riprese video a colori o in bianco e nero, possono essere dotate di brandeggio e di zoom ottico e sono collegate agli apparati nella sala

CED, che provvedono a digitalizzare e conservare i filmati in accordo con il presente regolamento.

4. I dati raccolti dalle dash cam, body cam e dalle videocamere dei droni vengono riversati sul server municipale, e seguono poi una gestione analoga a quella dei video.
5. (*Conservazione dei filmati di Videosorveglianza, telecamere a bordo auto e telecamere indossabili*). I dati vengono conservati per un periodo non superiore ai 7 giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o servizi, nonché nel caso in cui si deve rispondere ad una specifica richiesta investigativa dell'autorità giudiziaria o della polizia giudiziaria fatte salve esigenze di ulteriore conservazione.

L'eventuale allungamento dei tempi di conservazione deve essere valutato come eccezionale e comunque in relazione alla necessità derivante da un evento già accaduto o realmente imminente, oppure alla necessità di custodire o consegnare una copia specificamente richiesta all'autorità giudiziaria o di polizia giudiziaria in relazione ad un'attività investigativa in corso.

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

6. (*Conservazione dei dati relative alle targhe*). I dati relativi alle targhe vengono conservati per un periodo non superiore ai 7 giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione.
7. L'accesso ai sistemi è esclusivamente consentito al Comandante ed al personale autorizzato secondo le procedure di cui all'Art. 6.

Art. 11 - Specificità per Body Cam, Dash Cam e telecamere su droni

1. Gli operatori di Polizia Locale possono utilizzare, per i servizi a maggior rischio operativo, delle *Body Cam* e delle *Dash Cam* in conformità delle indicazioni dettate dal Garante della Privacy con nota 26 luglio 2016, prot. n. 49612, ed al parere preventivo pubblicato il 31/7/2014 (docweb 3423775) con cui sono state impartite le prescrizioni generali di utilizzo dei predetti dispositivi il cui trattamento dei dati (essendo stato abrogato l'articolo 53 del Codice) è ricondotto nell'ambito del D.lgs 51/2018 trattandosi di "dati personali direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela all'ordine e della sicurezza pubblica, nonché di polizia giudiziaria".
2. Gli operatori di Polizia Locale possono utilizzare le riprese tramite droni, per visualizzare aree non facilmente accessibili, o per avere una visione alternativa (aerea) dello scenario operativo (p.e. di un incidente). Qualora non sussistano finalità di sicurezza o 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.
3. Gli apparati "Telecamere modulari" (fototrappole) vengono posizionati secondo necessità, esclusivamente nei luoghi teatro di illeciti penali o amministrativi, quando questi ultimi non siano altrimenti accertabili con le ordinarie metodologie di indagine. Qualora non sussistano finalità di sicurezza o 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.
4. Le videocamere e le schede di memoria di cui sono dotate sono contraddistinte da un numero seriale che deve essere annotato in apposito registro recante il giorno, l'orario, i dati indicativi del servizio e la qualifica e nominativo del dipendente che firmerà la presa in carico e la restituzione. La scheda di memoria, all'atto della consegna ai singoli operatori, non deve contenere alcun dato archiviato.

5. Spetta all'ufficiale di Polizia Giudiziaria che impiega direttamente la pattuglia o in mancanza al Comandante o al capo Pattuglia di impartire l'ordine di attivazione dei dispositivi, in relazione all'evolversi degli scenari di sicurezza e ordine pubblico che facciano presupporre la criticità. Il medesimo dispone la cessazione delle riprese, che potranno essere riattivate ogni qualvolta lo stesso ne ravvisi la necessità.
6. Al termine del servizio gli operatori interessati, previa compilazione di un foglio di consegna, affidano tutta la documentazione video realizzata al funzionario, il quale provvede alla sua consegna presso il Comando.
7. Il sistema di registrazione dovrà essere attivato solo in caso di effettiva necessità, ossia nel caso di insorgenza delle situazioni descritte al comma 3.
8. Il trattamento dei dati personali effettuati con simili sistemi di ripresa deve rispettare i principi di cui all'art. 2 comma 3.

Art. 12 - Sicurezza dei dati

1. I dati oggetto di trattamento (registrazioni) sono custoditi ai sensi e per gli effetti del precedente art. 10. presso il CED, mentre nel Comando sono ubicate le attrezzature per la consultazione, a cui può accedere il solo personale autorizzato, secondo l'articolo 6.
2. La sede dove sono collocati i terminali è accessibile solamente al personale autorizzato in servizio del Corpo di Polizia Locale. I terminali richiedono automaticamente la password dopo un periodo di inattività
3. L'accesso al sistema di riconoscimento targhe, che è collocato presso il comune di S. Pietro in Cariano, avviene tramite una connessione criptata (connessione con Rete Privata Virtuale - VPN). Tutti gli altri accessi avvengono su rete privata dedicata. Eventuali altri accessi da remoto devono garantire un livello di sicurezza equivalente.
4. Inoltre, ciascun incaricato è dotato di proprie credenziali personali per l'accesso al sistema; le password devono avere una lunghezza minima di 8 caratteri, almeno un numero, un carattere minuscolo ed uno maiuscolo.
5. Il sistema consente di definire le operazioni consentite a ciascun utente, come per esempio configurare nuovo utente, visualizzare una registrazione, effettuarne una copia, effettuare un ripristino.
6. Le attività degli incaricati e dei Responsabili, (comprendendo con questo le operazioni di raccolta, modifica, consultazione, comunicazione, trasferimento, interconnessione e cancellazione dei dati), devono essere registrate sul sistema. Le informazioni registrate devono consentire di conoscere il tipo, la data e l'ora di tali operazioni e di identificare la persona che ha eseguito le operazioni e gli eventuali destinatari.
Il sistema deve conservare tale traccia delle operazioni effettuate, in modalità non modificabile dagli utenti; tale traccia (log) viene conservata per la durata di (almeno) **un anno**.
7. L'impiego di opportune protezioni sulle attrezzature di registrazione digitale impedisce di rimuovere il disco rigido su cui sono memorizzate le immagini.
8. Una copia di riserva dei dati viene tenuta presso la sala CED del comune.

Art. 13 - Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, di un trattamento, i dati personali sono:
 - a. distrutti;
 - b. ceduti ad altro titolare purché destinati ad un trattamento compatibile agli scopi per i quali i dati sono raccolti;
 - c. conservati per fini esclusivamente istituzionali.

2. La cessione dei dati in violazione di quanto previsto dal comma precedente o di altre disposizioni di legge in materia di trattamento dei dati personali determina la loro inutilizzabilità, fatta salva l'applicazione di sanzioni disciplinari ed amministrative, e, ove previsto dalla vigente normativa, l'avvio degli eventuali procedimenti penali.

Art. 14 - Valutazione di Impatto sulla protezione dei dati

1. In ossequio al disposto di cui all'art. 35, Paragrafo 3, lett. c), RGPD, nonché del provvedimento del Garante n. 467 dello 11 ottobre 2018, l'Ente procederà ad una valutazione dell'impatto sui rischi per le libertà ed i diritti degli interessati, causato dai trattamenti descritti in questo regolamento.

CAPO IV - DIRITTI E LIMITI NEL TRATTAMENTO DEI DATI, INFORMATIVA E VALUTAZIONE DI IMPATTO

Art. 15 - Diritti dell'interessato

1. In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto:
 - a. di conoscere l'esistenza di trattamenti di dati che possono riguardarlo, del periodo di conservazione degli stessi;
 - b. di essere informato sugli estremi identificativi del titolare (ed eventualmente del responsabile del trattamento) ed i dati di contatto del responsabile della protezione dei dati, oltre che sulle finalità e le modalità del trattamento dei dati;
 - c. 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;
 - d. di proporre reclamo a un'autorità di controllo;
 - e. di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21, RGPD.
2. È consentito solo all'Autorità Giudiziaria e alla Polizia Giudiziaria di acquisire copia delle immagini. Non è pertanto possibile fornire copia delle immagini direttamente ai cittadini.
In presenza di un fatto reato, il cittadino può, entro il termine di 24 ore, richiedere il blocco delle immagini in attesa che la forza di Polizia presso cui verrà proposta denuncia querela faccia apposita richiesta.
3. Le istanze sono presentate nei modi previsti dalla legge al titolare del trattamento. Nel caso di richiesta di blocco, l'interessato dovrà provvedere ad indicare:
 - a. il luogo, la data e la fascia oraria della possibile ripresa;
 - b. ogni ulteriore elemento utile all'identificazione dell'interessato;
 - c. l'eventuale presenza di accompagnatori al momento della possibile ripresa;
4. 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.
5. Nell'esercizio dei diritti di cui al comma 1, l'interessato può conferire per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.
6. Le istanze di cui al presente articolo possono essere presentate al protocollo comunale o trasmesse mediante lettera raccomandata, o negli altri modi previsti dalla legge, al titolare o al

responsabile del trattamento, i quali dovranno provvedere in merito entro e non oltre quindici giorni.

7. Nel caso di diniego all'istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Art. 16 - Informativa

1. Per i trattamenti di cui all'art. 10.1.a e 10.1.b, (videosorveglianza e riconoscimento targhe) gli interessati devono essere informati che stanno per accedere o che si trovano in una zona video sorvegliata, e dell'eventuale registrazione, mediante un modello semplificato di informativa "minima", riportato in *fac-simile* nell'allegato n. 1 del Provvedimento in materia di videosorveglianza del Garante per la Protezione dei dati Personali del 08/04/2010. Inoltre, per questi trattamenti:
 - a. 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.
 - b. In presenza di più telecamere, in relazione alla vastità dell'area ed alle modalità delle riprese, sono installati più cartelli.
 - c. L'Ente, in particolare, si obbliga ad affiggere la richiamata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere, su cui è riportata la seguente dicitura: "Area video sorvegliata – la registrazione è effettuata dal Comune di Negrar di Valpolicella, per fini di sicurezza urbana, incolumità e ordine pubblico".
2. L'informativa contenente tutti gli elementi di cui all'art. 13 del RGPD (cosiddetta informativa estesa), con particolare riguardo alle finalità ed all'eventuale conservazione sarà affissa in bacheca o in locali attigui alle aree video sorvegliate, e resa disponibile all'utenza senza oneri, nonché pubblicata sul sito internet dell'Ente. Detta informativa verrà tenuta aggiornata con eventuali successive variazioni o incrementi dimensionali dell'impianto stesso e dell'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, con un preavviso di giorni dieci.
3. Per i trattamenti di cui all'art. 10.1.c (telecamere per auto), le auto che trasportano le telecamere devono esporre una segnaletica equivalente a quella per la videosorveglianza.
4. Per i trattamenti di cui all'art. 10.1.d (telecamere personali), l'informativa avviene come segue:
 - a. la telecamera è normalmente spenta, e tenuta in evidenza (per esempio appesa al petto o al braccio);
 - b. quando l'agente riceve l'ordine di accenderla, deve avvertire l'interessato a voce; la telecamera deve avere una luce lampeggiante;
 - c. al termine della registrazione, la telecamera deve essere portata al Comando e le foto devono essere scaricate.
5. Per i trattamenti di cui all'art. 10.1.e (droni), l'area soggetta a ripresa deve essere delimitata con una segnaletica equivalente a quella per la videosorveglianza.

Art. 17 - Limiti alla utilizzabilità di dati personali

1. I trattamenti di cui all'articolo 10 non prevedono, in nessun caso, una valutazione del comportamento degli interessati fondato unicamente su un trattamento completamente automatizzato.

Art. 18 - Danni cagionati per effetto del trattamento di dati personali

1. Chiunque subisca un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento ai sensi delle disposizioni di cui all'art. 82, RGPD.
2. Il titolare o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
3. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2, RGPD.

Art. 19 - Comunicazione

1. La comunicazione di dati personali da parte dell'Ente ad altri soggetti pubblici è ammessa quando risulti comunque necessaria per lo svolgimento delle funzioni istituzionali e può essere iniziata se è decorso il termine di 45 giorni dal ricevimento della richiesta, salvo diversa determinazione, anche successiva, del Garante. Sono fatti salvi gli altri casi previsti dalla legge.
2. La comunicazione di dati personali da parte dell'Ente a privati o ad enti pubblici economici è ammessa unicamente quando prevista da una norma di legge.

CAPO V - TUTELA AMMINISTRATIVA E GIURISDIZIONALE: NORME FINALI

Art. 20 - Tutela

1. Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli art. 77 e seguenti, RGPD ed agli artt. 37 e seguenti del D.lgs 51/2018.
2. In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4-6 della legge 7 agosto 1990, n. 241, è il Comandante della Polizia Locale, così come individuato dal precedente art. 6.

Art. 21 - Provvedimenti attuativi

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

Art. 22 - Norma di rinvio

1. Per quanto non disciplinato dal presente Regolamento si rinvia al Regolamento UE 2016/679 (e al conseguente D.lgs 101/2018) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e al 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 e perseguimento di reati o esecuzione di sanzioni penali, nonché ai provvedimenti generali sulla videosorveglianza approvati dall'Autorità garante per la protezione dei dati personali

Art. 23 - Pubblicità del Regolamento

1. Copia del presente Regolamento, a norma dell'art. 22 della legge 7 agosto 1990 n. 241 e successive modificazioni ed integrazioni, sarà tenuta a disposizione del pubblico perché ne possa prendere visione in qualsiasi momento.
2. Copia dello stesso sarà altresì pubblicata sul sito internet del Comune.

Art. 24 - Entrata in vigore

1. Il presente Regolamento ai sensi dell'art. 54 del vigente Statuto comunale venga pubblicato all'Albo Pretorio, unitamente alla deliberazione di approvazione, per 15 giorni consecutivi; il regolamento, divenuta esecutiva la deliberazione di approvazione, dovrà essere ripubblicato all'albo pretorio per giorni 15 consecutivi. Entrerà in vigore il quindicesimo giorno successivo alla pubblicazione all'albo pretorio.