

FENIVA SRL

Security, Surveillance, Voice&Data Provider

- DOCUMENTO RISERVATO -

FENIVA S.r.l.  
Sede Legale V. Tasso 7 10121 TORINO  
Show Room C.so R. Parco 20 Bis/B 10153 TORINO  
Tel. +39 011 852 559  
Tel. +39 011 198 207 72  
<http://www.feniva.eu>

SPETT.le Comune di CANDIOLO  
ALLA C.A. COMANDANTE Polizia Locale

OGGETTO: Estratto con DPIA Impianto CCTV Comune CANDIOLO (TO)

Torino,

Egr. COMANDANTE,

Con la presente sono ad allegare alla presente l'Estratto con DPIA Impianto CCTV Comune Candiolo (TO).

Ringraziando per averci interpellato,

Con deferenza,

**Alessandro Oliva**  
IT Engineer – DPO - Feniva srl  
T +39 011 852559  
C.so R.Parco 20Bis 10153 Torino



**Alessandro Oliva**

**Privacy Officer**

Certificato TUV Italia al n\* CDP\_252\_V

**Settore di specializzazione: Videosorveglianza**  
Schema CDP Sviluppato in accordo alla ISO/IEC 17024:2012



**aicq  
sicev**

**Alessandro Oliva**

**Auditor A-ISDP©10003:2018 INVEO**

Cert.N.47 AICQ-SICEV A-ISDP©10003:2018

**Valutatore Privacy UNI 11697:2017**

Cert. N.53 UNI 11697:2017 - UNI EN ISO/IEC 17065:2015

# Estratto di Valutazione

L'impianto di videosorveglianza comunale, servizio della Polizia Locale indispensabile ai fini di Sicurezza e Tutela dei cittadini, del territorio, del bene pubblico, è stato l'oggetto di analisi per il trattamento dei dati nel periodo intercorso nell'annualità 2020.

L'analisi, la raccolta, l'osservazione dei sistemi di trattamento di immagini c.d. "videosorveglianza" sono state rivolte verso quattro aree e settori ben definiti:

- Le caratteristiche tecniche dei sistemi in uso
- Le attività amministrative di contesto/uso (Regolamenti, Procedure, Accesso interno/esterno ai dati di pertinenza)
- Il modello utilizzato nella progettualità e finalità per il raggiungimento del fine istituzionale di tutela della Sicurezza della cittadinanza e del bene pubblico
- tipologia dei Dati Personali in uso con valutazione del trattamento dei dati personali in termini di impatto e rischi per la persona.

Le quattro aree rappresentano l'atto di supporto ed estensione alla tecnologia per la sicurezza della cittadinanza e Tutela del bene pubblico. Compito istituzionale a cura del Corpo di Polizia Locale per cui, il trattamento dei dati si estende in coordinamento con le altre forze sul territorio e dei comuni limitrofi.

Attraverso l'analisi tecnica dei sistemi e componenti [l'insieme di telecamere, ponti radio, server immagini, server di backup] sono state rilevate le caratteristiche, le peculiarità nel funzionamento e la loro resilienza in caso di evento straordinario. Delineando in questa maniera la valutazione nell'insieme di accessibilità e resilienza ai dati personali e corretto trattamento.

L'analisi delle attività amministrative [procedure, istanze all'accesso dati, organizzazione ed organigramma, nomina delle varie figure] ha posto l'attenzione nella verifica e valutazione delle funzioni, dei ruoli [es. Responsabile ed incaricati] che su indicazione del Titolare, utilizzano quotidianamente il complesso tecnologico dei sistemi esaminati.

La progettualità, lo sviluppo e le implementazioni sul territorio del sistema tecnologico, in articolazione con le altre forze dell'ordine presenti sul territorio [in sviluppo e studio per la prassi del "Patto di Sicurezza con la Prefettura di competenza"] ha valutato ed esaminato quanto siano stati osservati i principi e concetti di "privacy by design e privacy by default" all'interno del contesto tecnologico; questo per valutare i termini di rispetto del trattamento dei dati, la riservatezza

nell'accesso ed il trattamento dei medesimi. La rappresentazione dei dati personali, sono la raffigurazione dei medesimi in forma di immagini statiche o video in movimento che dettagliano la presenza, le relazioni tra persone, mezzi e cose nel contesto cittadino.

Il Sistema di videosorveglianza di questo comando non ha in uso la cattura dell'audio [senza rilevazione live e recording], rappresenta con immagini e video la caratteristica di documentare e recare nel contenuto:

- La figura di una o più persone nel contesto cittadino riprese dal sistema di telecamere
- La figura, nei numeri e lettere che rappresentano le targhe di immatricolazione di veicoli a sistema europeo
- Il comportamento di una o più persone nell'ambito delle inquadrature. **Escludendo** in tal senso la c.d. “analisi intelligente” e la predizione del comportamento delle persone, aspetto di notevole impatto per la libertà personale.

E' importante sottolineare quanto, per le dovute finalità istituzionali di “Tutela del Territorio e Sicurezza delle persone”, il posizionamento e le inquadrature del sistema di telecamere sia stato opportunamente osservato, inquadrando esclusivamente porzioni di aree pubbliche, escludendo appositamente con precise prescrizioni, l'inquadratura di aree private atte a pregiudicare il comportamento legittimo nella sfera personale privata [es. abitazioni].

Il sistema opportunamente segnalato attraverso l'*informativa minima* su tutto il territorio, c.d. cartellonistica, atta riportare nella sua correttezza i riferimenti e le informazioni previste dalla Normativa europea GDPR|Normativa “codice Privacy”|Normativa “Codice di Videosorveglianza”, è presente con sufficiente ed ampia copertura su tutto il territorio comunale.

Appurato il corretto ruolo di informazione e comunicazione alla cittadinanza, oltre che alle persone in transito a vario titolo sul territorio comunale, è riscontrata la presenza di atti amministrativi [c.d. procedure e documentazioni scritte] che risultano indispensabili per una corretta gestione ed accesso ai dati, oltre che alla gestione delle “istanze di accesso” di tipo interno od esterno [della cittadinanza o di altre forze dell'ordine]. La gestione amministrativa del sistema di videosorveglianza rispecchia correttamente il concetto di “Accountability” [responsabilizzazione], operando attraverso la tracciatura di tutte le attività di trattamento dei dati personali che sono presenti all'interno delle immagini del sistema di videosorveglianza.

L'insieme di queste documentazioni e procedure, che devono essere costantemente verificate ed aggiornate, supportano quotidianamente e correttamente l'operato degli incaricati al trattamento per un regolare svolgimento del loro servizio.

Altresì, tale documentazione supporta il Responsabile dell'Area Vigilanza nel verificare e riportare periodicamente al Titolare, circa la qualità | sicurezza del trattamento e la corretta resilienza dei dati gestiti, e predispone al corretto comportamento di “Accountability” nel rispetto del trattamento dei dati personali attraverso il sistema di videosorveglianza.

Il trattamento dei dati personali, attraverso l'utilizzo del sistema di videosorveglianza, per le sue funzionalità è proporzionale e legittimo all'interesse del trattamento in relazione delle finalità istituzionali. Il concetto di proporzionalità esaminato, pertiene non per il rapporto numerico nella presenza di telecamere per metro quadro, ma di quanto impatta nella realtà cittadina il suo contenuto di ripresa, senza che siano raccolti ed estrapolati dati ai fini di profilazione, di comportamento o predittivi del comportamento. La proporzionalità delle riprese, non limitano il movimento di una persona, caratteristica per la quale l'impatto ed il rischio sarebbero elevati, ma ne preservano la libertà fintanto che si tratta di un comportamento nel perimetro della legalità e correttezza. Eventuali comportamenti scorretti nella gestione delle immagini, ad esempio illecita diffusione od errata estrazione, potrebbero assumere valori morali in termini di costo di vite umane, troppo alto rispetto alla finalità istituzionale da perseguire.

La difesa dei sistemi [intesa come difesa del dato in trattamento] posta nelle misure di sicurezza implementate | organizzate e quelle poste in implementazione, soddisfano il rapporto di qualità nel trattamento dei dati per la loro esattezza | resilienza | correttezza | liceità che, adeguatamente analizzate, rispecchiano la presenza e consapevolezza del Titolare e del Responsabile dei concetti “privacy by design e privacy by default” contenuti anche in normativa.

La valutazione tecnica del Rischio, nei termini di impatto per la libertà ed incolumità della persona a cui sono riferiti i dati personali, ha preso in esame oltre ai classici rapporti di probabilità | gravità, anche la capacità di resilienza ed analisi della medesima, nel mitigare il Rischio per contrastare l'avversità opponente rappresentata da eventuali inservibilità od esfiltrazioni indebite dei dati.

La valutazione positiva, per cui se ne gode il risultato di calcoli da osservazione nel medio periodo, detiene un sufficiente rapporto di valore, che dovrà e potrà essere aumentato, attraverso la continua formazione del personale incaricato al trattamento, attraverso l'aggiornamento | l'addestramento | la formazione continua, raggiungendo in tal modo, una crescente consapevolezza dei sempre più emergenti rischi nell'affidabilità e sviluppo tecnologico. Attraverso il riconoscimento del comportamento delle persone particolarmente interessate [social engineering], il riconoscimento dei sistemi e tecnologie in funzione del rischio, il riconoscimento della corretta gestione, il personale incaricato sarà sempre e maggiormente in grado di poter scongiurare indebiti accessi od esfiltrazioni di dati personali rappresentati nelle immagini statiche o video in movimento.

La valutazione positiva, nell'attività di trattamento dei dati personali [costituito dalle riprese delle telecamere di videosorveglianza sul territorio comunale] non rappresenta l'insieme dei permessi o infallibilità dei sistemi, ma raffigura l'insieme degli avvertimenti|delle misure|delle attività di mitigazione del rischio, che nel tempo devono essere periodicamente verificate e che si possono presentare in questo contesto tecnologico, in grado di adempiere in maniera corretta non soltanto al servizio di tutela istituito dalla Polizia Locale per la cittadinanza, ma rappresentare il corretto trattamento dei dati atti a proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.