# Informazioni sulla PIA

## Nome della PIA
Videosorveglianza Innovativa

## Nome autore
Fazio Giovanni

## Nome valutatore
Gilardoni Federico

## Data di creazione
19/02/2019

# Contesto

## Panoramica del trattamento

### Quale è il trattamento in considerazione?
All'interno del Parco Tokamachi vengono installate n.6 telecamere e relativo sistema di analisi immagini di tipo innovativo. Tale sistema permette (su n.2 telecamere in modo diretto, e per le altre telecamere in modo centralizzato) di effettuare le seguenti elaborazioni automatizzate:

- face-recognition (riconoscimento automatico di persone)
- loitering (riconoscimento automatico di situazioni di "bighellonaggio" da parte di persone)
- rilevamento automatico di abbandono oggetti
- rilevamento automatico di furto di oggetti
- tripwire (rilevamento automatico di attraversamento linea)

Si tratta di plugin software che consente alla telecamera di rilevare volti, persone, oggetti e, di conseguenza, generare notifiche.
Gli utilizzatori di questi plugin di videoanalisi sono:
- Operatori dipendenti dei Sistemi Informativi (Dirigente, Funzionario e/o facenti funzioni)
- Polizia Locale del Comune di Como (Comandante, Funzionari, Ufficiali e personale di centrale operativa)

L'accesso ai dati rilevati può essere effettuato da A2A Smart City in soli 2 casi:

- In fase di installazione, test e collaudo del sistema
- In fase di manutenzione correttiva a seguito di segnalazione di malfunzionamento

### Quali sono le responsabilità connesse al trattamento?
Il Titolare del Trattamento è il Sindaco del Comune di Como.
Il Responsabile del Trattamento è il Comandante della Polizia Locale, Dott. Donatello Ghezzo;
Il Sub-Responsabile del Trattamento è il Dirigente Sistemi Informativi, Ing. Giovanni Fazio;
Addetti delegati (ex-incaricati) così come sovradettagliato;
Il Responsabile della Protezione dei Dati (DPO), Dott. Federico Gilardoni

### Ci sono standard applicabili al trattamento?
Dentro il Comune di Como ad oggi non esistono standard applicabili al trattamento che si informa agli standard previsti per i trattamenti automatizzati di dati in materia di sicurezza.

# Dati, processi e risorse di supporto

## Quali sono i dati trattati?

i dati trattati sono:

- immagini riprese dalle n.6 telecamere
- foto segnaletiche di individui da ricercare nell'area coperta dalle telecamere.

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

Le immagini riprese dalla telecamere sono memorizzate per 7 gg. sul server dedicato, installato presso la Sala Server comunale.

La Sala Server è dotata di accesso controllato tramite badge, e sistema di videosorveglianza interno. L'accesso fisico alla Sala Server è consentito solo al personale dei Sistemi Informativi.

Le immagini possono essere visualizzate solo dal personale che svolge attività di indagini di Polizia Giudiziaria tramite n.2 PC client individuati in accordo con il Comandante della PL. Sui suddetti client vi è installato il software AxxonNext che consente di visualizzare le immagini sia in tempo reale che registrate ed è inoltre possibile, tramite configurazione ad hoc del profilo, di accedere alle funzioni avanzate di videosorveglianza.

L'accesso al Server del sistema, piuttosto che al client in Sala Operativa avviene con username/password debitamente profilati.

Le credenziali di accesso sono "personali" e vengano assegnate agli operatori di Polizia Locale indicati dal Responsabile dal Trattamento dei Dati.

Le politiche di sicurezza relative alle credenziali prevedono una scadenza delle password ogni 3 mesi e la non accettazione di password facilmente identificabili.

## Quali sono le risorse di supporto ai dati?

I dati delle telecamere sono ospitati a bordo del server Cloud IVS 3000 SCR che ne gestisce l’accesso, lo storage e la fruizione dei contenuti video. I flussi video sono salvati in load balancing su dischi in modalità RAID 5 per consentire un eventuale ripristino in caso di guasto di un HDD senza interruzione di servizio.

# Principi Fondamentali

# Proporzionalità e necessità

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

Finalità del trattamento:
consentire all nucleo di PG della Polizia Locale di individuare persone oggetto di indagine e/o scomparse al passaggio nell'area sottoposta a controllo; consentire di individuare automaticamente situazioni sospette (loitering), potenzialmente pericolose (abbandono di oggetti) o rilevare automaticamente furti di oggetti o ingressi/uscite da aree di interesse per indagini.
Le finalità di cui sopra sono specifiche, esplicite e legittime in quanto relative al raggiungimento e mantenimento di un buon livello di sicurezza pubblica reale e percepita.

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

Legge 23 aprile 2009 n. 38, art. 6, commi 7 e 8;
Direttiva 680/2016;
Regolamento UE 679/2016, art. 6;
D.Lgs. 10 agosto 2018 n. 101, art 2-octies;
Regolamento Comunale per l’utilizzo di impianti di videosorveglianza del territorio.

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

le foto segnaletiche degli individui da ricercare saranno memorizzate il solo tempo strettamente necessario all'indagine in corso, sotto la responsabilità del Comandante della Polizia Locale.
Le immagini resteranno registrate solamente per 7 gg, come da Regolamento comunale sulla Videosorveglianza. Solo in casi eccezionali potranno essere mantenute su esplicita richiesta della magistratura.

### I dati sono esatti e aggiornati?

I dati sono memorizzati nei limiti consentiti dalla legge e sovrascritti.

### Qual è il periodo di conservazione dei dati?

il periodo previsto di 7 gg. per la memorizzazione delle immagini sul server è ritenuto congruo per ipotizzare un flusso procedimentale standard che preveda la raccolta di una denuncia di un fatto da parte di una delle forze di polizia, l'attivazione dell'indagine, la richiesta di utilizzo del sistema di videosorveglianza innovativa ed infine un ragionevole tempo di utilizzo del sistema in oggetto per l'effettuazione dell'indagine.

## Misure a tutela dei diritti degli interessati

### Come sono informati del trattamento gli interessati?

Con specifici cartelli installati nei pressi delle telecamere

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

Nessun consenso previsto

### Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

In merito al diritto di accesso è consentito previo contatto del RDP-DPO ed in virtù di quanto disciplinato dall'art. 15 RGPD.

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

Utilizzando i dati per motivi di pubblica sicurezza si esclude il diritto di rettifica ed oblio.

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

Previo contatto del RDP-DPO ed in virtù di quanto disciplinato dall'art. 15 RGPD.

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

Sono disciplinati dall'incarico ad hoc ex art. 28 RGPD.

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

Non è previsto alcun trasferimento di dati all'esterno dell'Unione Europea.

## Rischi

# Misure esistenti o pianificate

## Controllo degli accessi logici

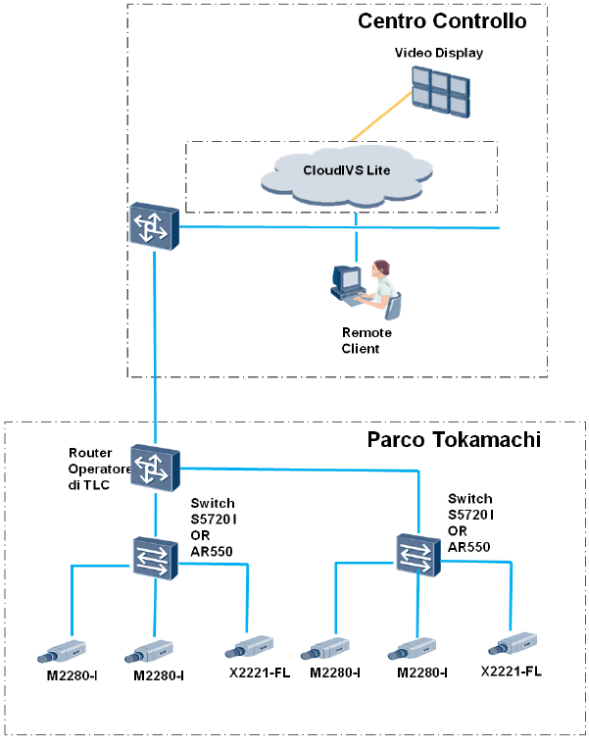
le credenziali vengono fornite personalmente ai singoli operatori di PG della Polizia Locale che ne debbano fare uso. Gli operatori sono indicati dal Comandante della Polizia Locale. Nessun invio di credenziali tramite e-mail, ma solo in modo diretto e personale.

## Tracciabilità

Il sistema tiene traccia dei log di accesso ed utilizzo del sistema.
Vengono inoltre tracciati i comandi relativi alla ricerca di video o immagini.

## Vulnerabilità

Il sistema di videosorveglianza è strutturato secondo la seguente architettura logica:




I dati delle telecamere sono ospitati a bordo del server Cloud IVS 3000 SCR che ne gestisce l'accesso, lo storage e la fruizione dei contenuti video.
Viene effettuato il buffering video, garantendo la completezza delle immagini.
Il server utilizza il sistema operativo Linux incorporato per garantire un funzionamento stabile 24 ore su 24, 7 giorni su 7, proteggendo il sistema dagli attacchi degli hacker e dai virus.

I metadati rilevati dalle video analisi (es. il dato di comparazione della face-recognition) vengono salvati in modo sicuro.

Il sistema operativo del Server verrà mantenuto aggiornato tramite WSUS.

**Limitazione Accesso Fisico**
il Client è installato su n.2 PC client all'interno della sede del Comando della Polizia Locale, individuati in accordo con il Comandante della PL. Tale Comando è presidiato h24 7/7 da agenti di Polizia Locale.
Il Server è posizionato in Sala Server del Comune di Como, in Via Vittorio Emanuele II. L'accesso alla sala è consentito solo tramite badge ai soli operatori dei Sistemi Informativi. La Sala è videosorvegliata da n.2 telecamere a raggi infrarossi.

## Lotta contro il malware

Installato Sophos a bordo del server. Tale Antivirus verrà mantenuto aggiornato dal server Sophos aziendale.

## Sicurezza dei canali informatici

Installato Sophos a bordo del server. Tale Antivirus verrà mantenuto aggiornato dal server Sophos aziendale.

## Politica di tutela della privacy

Il Responsabile della Protezione dei Dati del Comune di Como è il Dott. Federico Gilardoni. È prevista l'istituzione di una commissione per la gestione e il monitoraggio Privacy guidata dal RPD-DPO e composta da membri scelti dal Sindaco tra i Dirigenti e le P.O., detta commissione affronterà quanto prima la revisione del Regolamento e Politiche Privacy e del Regolamento sulla Videosorveglianza. Ad oggi il Comune di Como è in fase di adeguamento. Dopo l'adeguamento cartaceo è stato avviato anche l'adeguamento successivo.

## Gestione dei rischi

I Dati sono censiti così come i supporti utilizzati e sovradescritti. Il rischio e le misure vengono costantemente valutate e, una volta costituita la commissione, ne verranno previste di nuove con aggiornamenti continui delle stesse. Alla luce delle misure attuate e descritte il rischio è stimato come basso.

## Vigilanza sulla protezione dei dati

I Dati sono censiti così come i supporti utilizzati e sovradescritti. Il rischio e le misure vengono costantemente valutate e, una volta costituita la commissione, ne verranno previste di nuove con aggiornamenti continui delle stesse. Alla luce delle misure attuate e descritte il rischio è stimato come basso.

# Accesso illegittimo ai dati

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

Oltre all'usuale impatto relativo alla conoscenza della presenza di un individuo ad una certa ora/giorno/mese/anno nell'area oggetto della videosorveglianza, ulteriore impatto sull'interessato è quello relativo alla conoscenza di un'indagine in corso relativa all'interessato.

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

Accessi non autorizzati all'interno della rete dati aziendale.

## Quali sono le fonti di rischio?

Personale interno della Polizia Locale, personale dei Sistemi Informativi, amministratori di sistema, personale di A2A incaricato della manutenzione.

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

Controllo degli accessi logici, tracciabilità, Lotta contro il malware, Sicurezza dei canali informatici.

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

Il rischio è contenuto, l'impatto è alto in termini di violazione delle libertà personali.

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

Bassa. Il personale dipendente del Comune di Como (Polizia Locale e Sistemi Informativi) che potenzialmente potrebbe violare la Privacy è istituzionalmente abituato a lavorare su dati personali e sensibili. Al momento nessun data breach è mai stato segnalato.

# Modifiche indesiderate dei dati

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

Lesione della libertà personale.

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

Minaccia fisica al personale dotato di credenziali per l'inserimento/modifica delle foto segnaletiche, hacker.

### Quali sono le fonti di rischio?

Individui ricercati dalle forze di polizia, hacker

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

Controllo degli accessi logici, tracciabilità.

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

Il rischio è contenuto, l'impatto è alto in termini di violazione delle libertà personali.

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

Bassa. Il personale dipendente del Comune di Como (Polizia Locale e Sistemi Informativi) che potenzialmente potrebbe modificare i contenuti delle foto segnaletiche deve essere limitato a pochi ufficiali della Polizia Locale, individuati dal Comandante.
il Personale dei Sistemi Informativi non deve poter effettuare inserimenti/cancellazioni/modifiche delle foto succitate.

## Perdita di dati

### Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Lesione della libertà personale.

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

Rottura del sistema o accesso non autorizzato.

### Quali sono le fonti di rischio?

Sinistro.

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

Sicurezza dei canali informatici, sicurezza fisica del data center comunale e rispetto normativo.

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

Bassa, la perdita dei dati significa non poter utilizzare questo canale per le indagini.

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

Bassa, i sistemi sono sufficientemente ridondati ed affidabili.

# Piano d'azione

## Principi fondamentali

Legge 23 aprile 2009 n. 38, art. 6, commi 7 e 8;
Direttiva 680/2016;
Regolamento UE 679/2016;
Direttiva UE 680/2016;
Direttiva UE 681/2016;
D.P.R. 15 gennaio 2018, n. 15;
D.Lgs. 10 agosto 2018 n. 101, in particolare l'art 2-octies;
Regolamento Comunale per l'utilizzo di impianti di videosorveglianza del territorio.

## Misure esistenti o pianificate

Revisione dei regolamenti comunali in materia di Privacy e Videosorveglianza

## Rischi

Definizione di una procedura in caso di rischio di Accesso Illegittimo, Modifiche Indesiderate e Perdita di Dati da parte del Titolare del Trattamento.