Comune di Bassano Romano

Provincia di Viterbo

DATA PROTECTION IMPACT ASSESSMENT

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

UTILIZZO DI IMPIANTI DI VIDEOSORVEGLIANZA,
FOTOTRAPPOLE, RILEVATORI DI INFRAZIONE SEMAFORICA
E SISTEMA UAS (DRONE)
IN AMBITO COMUNALE

Data creazione	22/06/2025
Data aggiornamento	10/12/2025
N. Revisione	2.0
Redatto da	DPO / Titolare

Sommario

Sommario 2
1. Informazioni sulla DPIA 5
1.1 Nome della DPIA 5
1.2 Registro delle revisioni 5
2. Premessa 6
2.1 Scopo del documento 6
2.2 Visibilità del documento 6
2.3 Riferimento al Registro dei trattamenti 6
2.4 Definizioni, acronimi e abbreviazioni 6
3. Contesto 8
3.1 Panoramica del trattamento 8
3.1.1 Qual è il trattamento in considerazione? 8
3.1.2 Quali sono le responsabilità connesse al trattamento? 8
3.1.3 Ci sono standard applicabili al trattamento? 8
3.1.4 Trattamento mediante sistema UAS (Drone DJI Air 3S) 9
3.1.5 Trattamento mediante fototrappole mobili (Ekiller F4) 9
3.1.6 Trattamento mediante rilevatori di infrazione semaforica (Autosc@n RED) 10
3.2 Dati, processi e risorse di supporto 11
3.2.1 Quali sono i dati trattati? 11
3.2.2 Qual è il ciclo di vita del trattamento dei dati? 11
3.2.3 Quali sono le risorse di supporto ai dati? 12
4. Principi fondamentali 13
4.1 Proporzionalità e necessità 13
4.1.1 Gli scopi del trattamento sono specifici, espliciti e legittimi? 13
4.1.2 Quali sono le basi legali che rendono lecito il trattamento? 13
4.1.3 I dati raccolti sono adeguati, pertinenti e limitati (minimizzazione)? 13
4.1.4 I dati sono esatti e aggiornati? 13
4.1.5 Qual è il periodo di conservazione dei dati? 13
4.2 Misure a tutela dei diritti degli interessati 13
4.2.1 Come sono informati del trattamento gli interessati? 13
4.2.2 Come si ottiene il consenso degli interessati? 13
4.2.3 Come esercitano gli interessati i diritti di accesso e portabilità? 13
4.2.4 Come esercitano gli interessati i diritti di rettifica e cancellazione? 14
4.2.5 Come esercitano gli interessati i diritti di limitazione e opposizione? 14
4.2.6 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza? 14
4.2.7 In caso di trasferimento di dati fuori dall'UE? 14
5. Rischi 15
5.1 Criteri di valutazione del rischio 15

5.2 Misure esistenti o pianificate 15
5.2.1 Anonimizzazione 15
5.2.2 Controllo degli accessi logici e tracciabilità 15
5.2.3 Sicurezza dei documenti cartacei 15
5.2.4 Protezione contro malware e vulnerabilità 15
5.2.5 Crittografia 15
5.2.6 Minimizzazione dei dati 16
5.2.7 Archiviazione e backup 16
5.2.8 Controllo degli accessi fisici 16
5.2.9 Sicurezza dell'hardware 16
5.2.10 Manutenzione 16
5.2.11 Sicurezza dei canali informatici 16
5.2.12 Politica di tutela della privacy 16
5.2.13 Misure di sicurezza specifiche 16
5.3 Accesso illegittimo ai dati 16
5.3.1 Impatti potenziali 17
5.3.2 Principali minacce 17
5.3.3 Fonti di rischio 17
5.3.4 Misure di mitigazione 17
5.3.5 Valutazione 17
5.4 Modifiche indesiderate dei dati 17
5.4.1 Impatti potenziali 17
5.4.2 Principali minacce 17
5.4.3 Fonti di rischio 17
5.4.4 Misure di mitigazione 17
5.4.5 Valutazione 17
5.5 Perdita di dati 17
5.5.1 Impatti potenziali 17
5.5.2 Principali minacce 17
5.5.3 Fonti di rischio 17
5.5.4 Misure di mitigazione 18
5.5.5 Valutazione 18
5.6 Riepilogo della valutazione dei rischi 18
6. Esito della valutazione d'impatto 19
7. Parere del Responsabile della Protezione dei Dati (DPO) 20
Allegato 1 – Informazioni tecniche sul sistema di videosorveglianza 21
A. Impianto di videosorveglianza fisso 21
Elenco dei punti di installazione 21
B. Fototrappole mobili 22
C. Sistema UAS (Drone) 22

D. Rilevatori di infrazione semaforica (Autosc@n RED) 23

1. Informazioni sulla DPIA

1.1 Nome della DPIA

Impianto di videosorveglianza comunale, fototrappole mobili, rilevatori di infrazione semaforica Autosc@n RED e sistema UAS (Drone) – Comune di Bassano Romano.

Titolare del trattamento	Comune di Bassano Romano
Data creazione	22/06/2025
Data ultimo aggiornamento	10/12/2025
N. Revisione	2.0
Motivo della revisione	Integrazione sezione UAS (Drone DJI Air 3S), fototrappole Ekiller F4 e rilevatori Autosc@n RED; correzione periodo di conservazione; aggiornamento normativo; inserimento parere DPO e sezione conclusiva.

1.2 Registro delle revisioni

Rev.	Data	Autore	Descrizione
1.0	22/06/2025	DPO	Prima emissione
2.0	10/12/2025	DPO	Integrazione UAS, fototrappole, Autosc@n RED, correzioni, aggiornamento normativo

2. Premessa

2.1 Scopo del documento

La presente Valutazione d'Impatto sulla Protezione dei Dati (DPIA) è redatta ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito «GDPR»). La DPIA si rende necessaria ogniqualvolta dal trattamento possa conseguire un rischio elevato per i diritti e le libertà delle persone interessate, anche durante un trattamento già in corso di esecuzione, qualora si verifichi un mutamento nelle finalità o una modifica dei dati stessi che comporti una maggiore percentuale di rischio.

La valutazione di impatto è sempre richiesta, in particolare, in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico (art. 35, par. 3, lett. c) del GDPR) e negli altri casi indicati dal Garante con il provvedimento n. 467 dell'11 ottobre 2018.

Il modello della presente DPIA è stato estratto, senza rielaborazioni sostanziali, dallo strumento PIA progettato dalla Commission Nationale de l'Informatique et des Libertés (CNIL v. 2.3.0), autorità di controllo francese, esplicitamente validato e suggerito anche dal Garante per la protezione dei dati personali italiano.

2.2 Visibilità del documento

Il documento è principalmente indirizzato alle persone coinvolte nel lavoro di attuazione della normativa in materia di protezione dati, al DPO dell'Ente e alle autorità di controllo competenti.

2.3 Riferimento al Registro dei trattamenti

Il trattamento oggetto della presente DPIA è inserito nel Registro dei trattamenti dell'Ente ai sensi dell'art. 30 del GDPR. Ogni aggiornamento della presente valutazione deve essere riportato coerentemente nel Registro.

2.4 Definizioni, acronimi e abbreviazioni

Servizio	Utilizzo degli impianti di videosorveglianza fissi, delle fototrappole mobili, dei rilevatori di infrazione semaforica e del sistema UAS (Drone) attivati nel territorio del Comune di Bassano Romano.
Titolare del trattamento	Il Comune di Bassano Romano, ai sensi dell'art. 4, n. 7, del GDPR, cui competono le decisioni in ordine alle finalità e alle modalità del trattamento dei dati personali.
Responsabile del trattamento	Soggetto/Azienda fornitrice del Servizio, eventualmente nominata Responsabile del trattamento ai sensi dell'art. 28 del GDPR.
Interessato	La persona fisica cui si riferiscono i dati personali oggetto di trattamento, identificata o identificabile in modo diretto o indiretto.
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 (raccolta, registrazione, organizzazione, conservazione, consultazione, uso, comunicazione, cancellazione, distruzione, ecc.) ai sensi dell'art. 4, n. 2, del GDPR.
Rischio	Il prodotto tra la probabilità di ledere i diritti e le libertà delle persone fisiche e l'impatto su tali diritti e libertà che si produrrebbe ove la minaccia si dovesse verificare.
DPIA / PIA	Data Protection Impact Assessment (Valutazione d'Impatto sulla protezione dei dati).
GDPR / Reg. UE 2016/679	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.
UAS	Unmanned Aircraft System – Sistema aeromobile a pilotaggio remoto (Drone).

Fototrappola	Dispositivo mobile di videosorveglianza riposizionabile, impiegato per il contrasto di illeciti ambientali e reati itineranti.
Autosc@n RED	Sistema di rilevamento e sanzionamento automatico delle violazioni al semaforo rosso, mediante acquisizione di immagini e filmati dei veicoli che superano la linea di arresto. Piattaforma sviluppata dal Gruppo Maggioli.
VDS	Videosorveglianza.
DPO	Data Protection Officer – Responsabile della protezione dei dati, ai sensi degli artt. 37-39 del GDPR.

3. Contesto

3.1 Panoramica del trattamento

3.1.1 Qual è il trattamento in considerazione?

Il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza fissi (VDS), delle fototrappole mobili Ekiller F4, dei rilevatori di infrazione semaforica Autosc@n RED e del sistema UAS (Drone), attivati nel territorio dell'Ente, è operato dal Comune di Bassano Romano nella persona del Sindaco pro tempore e dei soggetti specificatamente autorizzati.

Per le immagini riprese e/o registrate nel Comune di Bassano Romano, il titolare dei dati è il Comune medesimo. Per le immagini riprese e/o registrate in altri Comuni eventualmente convenzionati, il titolare dei dati è il Comune convenzionato.

Le finalità di utilizzo degli impianti di videosorveglianza sono conformi alle funzioni istituzionali attribuite al Comune dalla legge 7 marzo 1986, n. 65 sull'ordinamento della Polizia Municipale, dallo statuto e dai regolamenti comunali, dalla direttiva Polizia 2016/680 attuata con D.Lgs. 18 maggio 2018, n. 51, nonché dal decreto-legge n. 14 del 20 febbraio 2017 convertito in legge n. 48 del 18 aprile 2017 e successive modificazioni.

Il trattamento dei dati personali mediante i sistemi di videosorveglianza è effettuato ai fini di:

- **tutela della sicurezza urbana e della sicurezza pubblica** – attività di prevenzione, indagine, accertamento e perseguimento di atti delittuosi, attività illecite ed episodi di microcriminalità, tutela dell'ordine, del decoro e della quiete pubblica;
- **tutela del patrimonio comunale** – vigilanza sull'integrità, conservazione e tutela del patrimonio pubblico e privato;
- **tutela della sicurezza stradale e controllo della circolazione dei veicoli** – monitoraggio della viabilità e dei flussi di traffico, accertamento delle violazioni del Codice della Strada tramite lettura targhe;
- **tutela ambientale e polizia amministrativa** – controllo di aree specifiche del territorio per prevenire e reprimere illeciti legati a fenomeni di degrado, discarica di materiale e sostanze pericolose o abbandono di rifiuti;
- **polizia giudiziaria** – prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nell'ambito delle attività di P.G.

3.1.2 Quali sono le responsabilità connesse al trattamento?

Le responsabilità connesse al trattamento sono ascrivibili alla gestione delle attività di accesso, salvataggio, archiviazione, nonché alle attività manutentive legate all'utilizzo degli impianti VDS, delle fototrappole, dei rilevatori Autosc@n RED e del sistema UAS.

Il trattamento effettuato mediante i sistemi tecnologici descritti potrebbe potenzialmente configurarsi come sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La presente analisi garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, alla libertà di circolazione nei luoghi pubblici o aperti al pubblico, nonché ai diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti.

3.1.3 Ci sono standard applicabili al trattamento?

L'attività di videosorveglianza e l'impiego delle fototrappole, dei rilevatori di infrazione semaforica e dell'UAS sono disciplinati dai seguenti provvedimenti:

- Provvedimento generale in materia di videosorveglianza del Garante dell'8 aprile 2010 (G.U. n. 99 del 29/04/2010);
- Linee guida sulla videosorveglianza negli enti locali dell'ANCI del 9 novembre 2010;
- Circolare del Ministero dell'Interno sui sistemi di videosorveglianza per i Comuni del 2 marzo 2012;
- Regolamento (UE) 2016/679 (GDPR);
- Decreto Legislativo 30 giugno 2003, n. 196, come modificato e integrato dal D.Lgs. 101/2018;
- Allegato 1 al provvedimento n. 467 dell'11 ottobre 2018 (G.U. n. 269 del 19 novembre 2018);

- Direttiva (UE) 2016/680, recepita con il D.Lgs. 51/2018;
- DPR 15 gennaio 2018, n. 15;
- Decreto-legge 20 febbraio 2017, n. 14, convertito con L. 18 aprile 2017, n. 48, e successive modificazioni;
- Linee guida EDPB 3/2019, versione 2.0 del 29 gennaio 2020, sul trattamento di dati personali attraverso dispositivi video;
- Regole per installare telecamere del 5 dicembre 2020, vademecum e FAQ del Garante del 3 dicembre 2020;
- Regolamento di esecuzione (UE) 2019/947 relativo a norme e procedure per l'esercizio di aeromobili senza equipaggio;
- Regolamento delegato (UE) 2019/945 relativo ai requisiti tecnici per i sistemi UAS;
- Regolamento ENAC UAS-IT e successive edizioni.

3.1.4 Trattamento mediante sistema UAS (Drone DJI Air 3S)

Il Comune di Bassano Romano, tramite il Corpo di Polizia Locale, utilizza un aeromobile a pilotaggio remoto (UAS) di tipo DJI Air 3S per lo svolgimento di riprese aeree finalizzate a specifiche attività istituzionali, in conformità alla normativa in materia di sicurezza urbana, polizia locale, polizia giudiziaria, tutela ambientale e protezione civile.

Le riprese avvengono in aree pubbliche e, in taluni casi, possono includere limitate porzioni di aree private visibili dall'alto, esclusivamente se strettamente pertinenti all'attività istituzionale svolta. Il dispositivo non effettua registrazione audio, né utilizza sistemi di riconoscimento facciale o tecniche di identificazione biometrica.

Le finalità del trattamento tramite UAS includono:

- attività di polizia giudiziaria ai sensi dell'art. 55 c.p.p. e L. 65/1986;
- attività di polizia stradale (art. 11 C.d.S.);
- attività di sicurezza urbana e tutela dell'ordine pubblico;
- documentazione di sinistri stradali, dissesti, frane, incendi, crolli o altri eventi emergenziali;
- accertamento di illeciti edilizi, paesaggistici e ambientali;
- attività connesse alla protezione civile locale;
- monitoraggio della corretta fruizione degli eventi pubblici ai fini di safety e security.

Non è consentito l'utilizzo dell'UAS per finalità diverse da quelle istituzionali. L'impiego è subordinato all'esistenza di un'esigenza istituzionale specifica, documentata tramite il Registro dei voli UAS.

Le immagini vengono trasferite dalla microSD del drone esclusivamente su postazioni informatiche del Comando della Polizia Locale, all'interno di volumi cifrati mediante algoritmi AES-256 (BitLocker o VeraCrypt). La microSD, dopo il trasferimento, è riformattata oppure custodita in busta sigillata in caso di rilevanza probatoria. Ogni operazione di accesso, copia o estrazione dati è annotata nel Registro degli accessi ai dati UAS.

3.1.5 Trattamento mediante fototrappole mobili (Ekiller F4)

Il Comune di Bassano Romano dispone di n. 2 fototrappole mobili di tipo Ekiller F4, sistemi di videosorveglianza mobile riposizionabili, utilizzati dal Corpo di Polizia Locale per il contrasto di reati itineranti e illeciti ambientali, in particolare l'abbandono illecito di rifiuti, nonché per attività di polizia giudiziaria ove necessario.

Le fototrappole Ekiller F4 presentano le seguenti caratteristiche tecniche rilevanti ai fini della protezione dei dati:

- sensore STARLIGHT 1/2.8" 2MP CMOS con risoluzione FullHD 1080p a 25 fps;
- codifica video H.265+ e H.264+ Triple-Stream;
- funzionalità Day/Night elettronica con WDR, HLC, BLC e 3DNR;
- ottiche intercambiabili (2,8 mm / 8 mm / 12 mm / 16 mm / 25 mm) per inquadrature da 5 m a 80 m con lettura targhe anche in notturna;
- crittografia AES-256 su microSD da 256 GB integrata;
- Digital Watermarking per garantire l'autenticità e la non alterazione delle registrazioni;

- Smart Detection: rilevamento oggetto abbandonato o rimosso, intrusione, attraversamento linea, motion detection;
- gestione da remoto in tempo reale tramite software VMS Ekiller su PC e App Mobile;
- autonomia della batteria al litio di circa 120 ore (estendibile con pacchi batteria aggiuntivi);
- grado di protezione IP66; temperatura operativa da -20°C a +50°C;
- dimensioni contenute (≤ 26x23x11 cm), peso massimo 5.490 g;
- gabbia in acciaio inox con catena da 2,5 m e 2 lucchetti antifurto;
- conformità dichiarata al GDPR da parte del produttore.

Le fototrappole non effettuano registrazione audio. Il posizionamento avviene secondo necessità operativa, nei luoghi teatro di illeciti ambientali o penali. L'utilizzo per l'accertamento di illeciti amministrativi è ammesso solo qualora non siano altrimenti accertabili con le ordinarie metodologie di indagine e nel rispetto del principio di minimizzazione.

Le finalità del trattamento tramite fototrappole includono:

- contrasto all'abbandono illecito di rifiuti e discariche abusive;
- prevenzione e repressione di atti di vandalismo e danneggiamento del patrimonio pubblico;
- attività di polizia giudiziaria e accertamento di illeciti penali e amministrativi;
- tutela ambientale e polizia amministrativa.

Le immagini registrate sono accessibili tramite il software VMS Ekiller e l'App Mobile, esclusivamente da personale autorizzato dotato di credenziali personali. La funzione di timeline intelligente e Autosave consente la navigazione diretta ai momenti rilevanti, riducendo i tempi di analisi. I dati sulla microSD sono protetti da crittografia AES-256 e ogni esportazione è tracciata.

I dati sono conservati per un periodo non superiore a 7 giorni, con possibilità di estensione fino a 90 giorni per esigenze investigative documentate. La microSD è riformattata al termine di ogni ciclo operativo o custodita in modo sicuro in caso di rilevanza probatoria.

3.1.6 Trattamento mediante rilevatori di infrazione semaforica (Autosc@n RED)

Il Comune di Bassano Romano dispone di n. 2 sistemi di rilevamento e sanzionamento automatico delle violazioni al semaforo rosso, modello Autosc@n RED, prodotti e gestiti dal Gruppo Maggioli nell'ambito della piattaforma Autosc@n integrata con il software gestionale Concilia.

Il sistema Autosc@n RED rileva, fotografa e identifica le targhe dei veicoli che superano la linea di arresto durante la fase di rosso del semaforo. Per ogni violazione il sistema acquisisce:

- n. 8 immagini per violazione, di cui 2 con riconoscimento ottico dei caratteri (OCR);
- n. 1 video della violazione;
- dati del transito: data, ora, luogo, direzione di marcia, numero di targa del veicolo.

Le caratteristiche tecniche rilevanti ai fini della protezione dei dati includono:

- mascheramento automatico dei dati sensibili nella scena ripresa a tutela della privacy di terzi;
- gestione delle fasi di integrazione, correzione e validazione dell'infrazione da parte dell'operatore autorizzato;
- ricerca del proprietario del veicolo presso la banca dati della motorizzazione DTTSIS;
- interfaccia nativa con il software Concilia per l'importazione automatica delle violazioni;
- produzione di statistiche sui transiti e sulle violazioni;
- archiviazione delle immagini con possibilità di modifica di luminosità e contrasto per migliorare la qualità di visualizzazione.

Modalità di erogazione del servizio. Il sistema Autosc@n RED è erogato in modalità Cloud tramite i data center del Gruppo Maggioli, localizzati in Italia e qualificati ACN (Agenzia per la Cybersicurezza Nazionale). L'Ente è sollevato dalla gestione dell'infrastruttura fisica (sicurezza, ridondanza, backup, recovery). I dati personali trattati attraverso la piattaforma restano all'interno del territorio italiano e non vengono trasferiti al di fuori dello Spazio Economico Europeo.

Responsabile del trattamento. Il Gruppo Maggioli / Concilia Service è nominato Responsabile del trattamento ai sensi dell'art. 28 del GDPR, con apposito contratto che disciplina la natura e le finalità

del trattamento, gli obblighi del responsabile, le misure di sicurezza, le modalità di restituzione e cancellazione dei dati al termine del servizio.

I dispositivi Autosc@n RED sono installati presso le seguenti intersezioni semaforiche:

- S.P. 40 inc. via XXIV Maggio
- S.P. 40 inc. via Sant'Andrea

3.2 Dati, processi e risorse di supporto

3.2.1 Quali sono i dati trattati?

I dati personali sono raccolti attraverso riprese video e captazione di immagini effettuate da: telecamere fisse installate in luoghi pubblici e aperti al pubblico e lungo le arterie stradali del territorio comunale; fototrappole mobili Ekiller F4 posizionate nei siti di interesse operativo; rilevatori di infrazione semaforica Autosc@n RED installati presso intersezioni semaforiche; sistema UAS DJI Air 3S per riprese aeree.

Gli impianti riprendono e registrano immagini che permettono di identificare in modo diretto o indiretto le persone riprese. Sono inoltre trattati i dati degli autoveicoli (numero di targa) e delle persone fisiche che circolano in prossimità dei dispositivi. I sistemi Autosc@n RED trattano specificamente immagini dei veicoli in transito, numeri di targa (anche tramite OCR), video delle violazioni e dati di contesto (data, ora, luogo). Il drone e le fototrappole non registrano audio e non effettuano trattamenti biometrici.

3.2.2 Qual è il ciclo di vita del trattamento dei dati?

Il ciclo di vita dei dati prevede le seguenti fasi: acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto, interconnessione, limitazione, pseudonimizzazione, cancellazione.

Videosorveglianza fissa. L'impianto consente riprese video e foto, diurne e notturne. È sempre in funzione e configurato per la registrazione continuativa. Le telecamere non sono dotate di microfono né di sensori biometrici. Le telecamere sono collegate alla sala di controllo del Comando di Polizia Locale. Le immagini sono visualizzate in tempo reale su monitor da personale autorizzato. Il sistema è a circuito chiuso, senza possibilità di accesso da remoto. Il salvataggio avviene su server dedicato presso il Comando.

Fototrappole Ekiller F4. Le immagini sono registrate su microSD crittografata AES-256 integrata nel dispositivo. L'accesso ai dati avviene tramite il software VMS Ekiller o l'App Mobile da parte del solo personale autorizzato con credenziali personali. Il Digital Watermarking garantisce l'integrità e l'autenticità delle registrazioni. La gestione da remoto in tempo reale consente il monitoraggio operativo senza necessità di recarsi fisicamente sul posto.

Sistema UAS. Il ciclo comprende: acquisizione delle immagini tramite drone, registrazione su microSD, trasferimento su volume cifrato AES-256 presso il Comando, annotazione nel Registro dei voli e nel Registro accessi dati, conservazione limitata e cancellazione al termine dei tempi previsti.

Rilevatori Autosc@n RED. Il ciclo comprende: acquisizione automatica delle immagini e del video al momento della violazione, lettura OCR della targa, trasmissione dei dati al cloud Maggioli, validazione dell'infrazione da parte dell'operatore autorizzato tramite la piattaforma Autosc@n, ricerca del proprietario del veicolo presso la banca dati DTTSIS, esportazione verso il software Concilia per l'emissione del verbale, conservazione per i termini di legge e cancellazione automatica.

Conservazione delle immagini. Le immagini del sistema VDS fisso e delle fototrappole sono conservate per un periodo ordinariamente non superiore a sette (7) giorni dalla rilevazione. Il periodo può essere esteso fino a 90 giorni per esigenze investigative documentate. Per le telecamere a tutela del solo patrimonio comunale, la conservazione non supera le 72 ore. Per il sistema UAS, la conservazione è di 72 ore per attività amministrative e per il tempo necessario alla conclusione del procedimento per attività di P.G. Per i rilevatori Autosc@n RED, le immagini e i video delle violazioni sono conservati per il tempo necessario alla definizione del procedimento sanzionatorio e degli eventuali ricorsi, in conformità alla normativa vigente.

Al termine del periodo stabilito, il sistema provvede in automatico alla cancellazione mediante sovra-registrazione, ove tecnicamente possibile.

Possono essere autorizzati all'accesso alla sala di controllo solo incaricati di servizi rientranti nei compiti istituzionali dell'Ente, nonché il personale addetto alla manutenzione, preventivamente individuato. L'accesso da parte di soggetti diversi è subordinato ad autorizzazione scritta e motivata e avviene in presenza di incaricati del Comune.

Gli autorizzati al trattamento sono gli unici dotati di credenziali di autenticazione personali. L'accesso ai sistemi è tracciato mediante log, con conservazione per un periodo non inferiore a sei mesi. L'accesso alla sala operativa è protetto da sistemi di sicurezza fisici e da armadio rack con serratura.

Il personale autorizzato può visionare le registrazioni esclusivamente per il perseguimento dei fini istituzionali:

- sulla base di denunce di atti criminosi, per l'inoltro delle fonti di prova all'autorità giudiziaria;
- sulla base di segnalazioni di atti criminosi accertate dagli organi di polizia in servizio;
- sulla base di atti criminosi rilevati direttamente dagli operatori nell'esercizio delle proprie funzioni;
- su richiesta specifica dell'autorità giudiziaria;
- su richiesta di organi o autorità espressamente autorizzati secondo norme di legge.

3.2.3 Quali sono le risorse di supporto ai dati?

Persone: Sindaco; Comandante della Polizia Locale; Agenti di Polizia Locale formati e autorizzati; operatori UAS abilitati.

Hardware e Software: infrastruttura HW e SW come da scheda tecnica allegata (Allegato 1); n. 2 fototrappole Ekiller F4 con software VMS Ekiller e App Mobile; n. 2 rilevatori Autosc@n RED con piattaforma Autosc@n in cloud Maggioli e software Concilia; n. 1 drone DJI Air 3S.

4. Principi fondamentali

4.1 Proporzionalità e necessità

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

Il trattamento si svolge nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche. L'utilizzo degli impianti comporta esclusivamente il trattamento di dati personali rilevati mediante riprese video e foto che interessano i soggetti e i mezzi di trasporto che transitano nelle aree sorvegliate.

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

La base giuridica è la necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri ai sensi dell'art. 6, par. 1, lett. e) del GDPR, nonché la necessità di eseguire un compito di un'autorità competente per le finalità di prevenzione, accertamento e perseguimento dei reati (art. 5 D.Lgs. 51/2018).

4.1.3 I dati raccolti sono adeguati, pertinenti e limitati (minimizzazione)?

In applicazione dei principi di minimizzazione di cui all'art. 5, par. 1, lett. c) del GDPR, tutti i sistemi sono configurati per ridurre al minimo l'utilizzazione di dati personali, limitando l'angolo di visuale e evitando immagini dettagliate quando non indispensabili. Le fototrappole Ekiller F4 sono dotate di Smart Detection che consente la registrazione solo in presenza di eventi rilevanti (motion detection, attraversamento linea, intrusione), contribuendo alla minimizzazione dei dati trattati. In ambito pubblico, la rilevazione non è estesa ad aree prive di rischi concreti. Gli impianti sono attivati solo quando altre misure risultino insufficienti o inattuabili.

4.1.4 I dati sono esatti e aggiornati?

I dati vengono aggiornati periodicamente, almeno su base annuale, e incrociati con le banche dati nazionali.

4.1.5 Qual è il periodo di conservazione dei dati?

Le immagini del sistema VDS fisso e delle fototrappole sono conservate per un periodo non superiore a **sette (7) giorni** dalla rilevazione. Decorso tale periodo, i dati sono sovrascritti automaticamente. Il periodo può essere esteso fino a 90 giorni per esigenze investigative e di polizia giudiziaria documentate, su richiesta dell'autorità prefettizia o giudiziaria.

Per le telecamere a tutela del solo patrimonio comunale, il periodo non supera le **72 ore**, fatte salve esigenze debitamente documentate.

Per il sistema UAS, la conservazione è di **72 ore** per attività amministrative e per il tempo necessario alla conclusione del procedimento per attività di P.G.

4.2 Misure a tutela dei diritti degli interessati

4.2.1 Come sono informati del trattamento gli interessati?

Gli interessati sono informati mediante:

- pubblicazione del regolamento comunale comprensivo dei dettagli sulle zone videosorvegliate sul sito web istituzionale;
- installazione di apposita segnaletica permanente (informativa breve) nelle aree in cui sono posizionate le telecamere fisse, collocata prima del raggio di azione di ogni telecamera;
- per le fototrappole mobili, apposizione di segnaletica informativa nell'area interessata al momento dell'installazione;
- informativa completa ai sensi degli artt. 12, 13 e 14 del GDPR, disponibile senza oneri sul sito web e nei locali dell'Ente.

L'informativa non è dovuta nel caso di utilizzo a scopo investigativo a tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati.

4.2.2 Come si ottiene il consenso degli interessati?

Il Titolare del trattamento è una pubblica amministrazione e non è tenuto all'acquisizione del consenso, ai sensi dell'art. 6, par. 1, lett. e) del GDPR.

4.2.3 Come esercitano gli interessati i diritti di accesso e portabilità?

Gli interessati possono rivolgersi al Titolare o al DPO ai sensi dell'art. 38, par. 4, del GDPR, mediante lettera raccomandata o PEC a bassanoromano@legalmail.it. In caso di richiesta di accesso alle immagini, l'interessato deve indicare luogo, data, fascia oraria, abbigliamento, accessori, accompagnatori, attività svolta e ogni ulteriore elemento utile all'identificazione. Il rilascio di copia avviene in formato elettronico comune, previo oscuramento dei dati di terzi (art. 15, par. 3 e 4 del GDPR).

4.2.4 Come esercitano gli interessati i diritti di rettifica e cancellazione?

Il diritto di rettificazione non è concretamente esercitabile data la natura intrinseca dei dati (immagini in tempo reale). Per la cancellazione, gli interessati possono contattare il Titolare, il DPO o il responsabile esterno tramite i canali indicati nell'informativa.

4.2.5 Come esercitano gli interessati i diritti di limitazione e opposizione?

Mediante i medesimi canali di contatto sopra indicati.

4.2.6 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza?

Il rapporto tra Titolare e responsabile esterno è disciplinato da contratto di appalto o comunicazione specifica, con allegato di nomina conforme all'art. 28 del GDPR. In particolare, il Gruppo Maggioli / Concilia Service, in qualità di Responsabile del trattamento per il servizio Autosc@n RED erogato in cloud, è vincolato da apposito contratto ex art. 28 del GDPR che disciplina le modalità di trattamento, le misure di sicurezza, gli obblighi di riservatezza e le procedure di restituzione e cancellazione dei dati.

4.2.7 In caso di trasferimento di dati fuori dall'UE?

I dati non vengono trasferiti al di fuori dello Spazio Economico Europeo (SEE). I sistemi Ekiller F4 archiviano i dati su microSD locale crittografata. Il sistema Autosc@n RED è erogato in cloud tramite i data center del Gruppo Maggioli, localizzati in Italia e qualificati ACN; i dati trattati restano pertanto all'interno del territorio nazionale. Nessun sistema prevede trasferimenti automatici verso server al di fuori dello SEE.

5. Rischi

5.1 Criteri di valutazione del rischio

La valutazione del rischio è effettuata sulla base di una matrice che combina la gravità dell'impatto potenziale con la probabilità che l'evento si verifichi:

Livello	Descrizione gravità
1 – Trascurabile	Impatto minimo, nessun danno significativo.
2 – Limitato	Disagio superabile senza difficoltà.
3 – Significativo	Danno rilevante superabile con difficoltà.
4 – Massimo	Danno irreversibile o molto difficilmente superabile.
Livello	**Descrizione probabilità**
1 – Trascurabile	Evento non prevedibile.
2 – Limitata	Evento poco probabile, misure adeguate.
3 – Significativa	Evento possibile, fonti di rischio con capacità note.
4 – Massima	Evento altamente probabile.

Matrice di rischio: il rischio è determinato dall'intersezione tra gravità e probabilità.

Grav. ↓ / Prob. →	1	2	3	4
1 – Trasc.	1	2	3	4
2 – Limit.	2	4	6	8
3 – Sign.	3	6	9	12
4 – Mass.	4	8	12	16

Legenda: Verde (1-2) = rischio accettabile; Giallo (3-4) = basso, monitoraggio; Arancione (6-9) = medio, azioni correttive; Rosso (12-16) = elevato, intervento immediato.

5.2 Misure esistenti o pianificate

5.2.1 Anonimizzazione

I dati particolari eventualmente rilevati vengono trattati in maniera riservata unicamente dal personale autorizzato. I dati sono resi anonimi ove possibile.

5.2.2 Controllo degli accessi logici e tracciabilità

- Postazione informatica dedicata con username e password personale per ogni operatore;
- Registrazione e tracciabilità degli accessi logici e delle operazioni;
- Credenziali a uso esclusivo, modificate ciclicamente; screensaver con reinserimento password;
- Disattivazione delle credenziali in caso di inutilizzo prolungato o perdita della qualifica;
- Per le fototrappole Ekiller F4: accesso tramite credenziali personali al software VMS e all'App Mobile, con tracciamento delle operazioni di visualizzazione e esportazione.

5.2.3 Sicurezza dei documenti cartacei

I documenti cartacei sono conservati garantendo riservatezza e non visibilità a terzi non autorizzati.

5.2.4 Protezione contro malware e vulnerabilità

- Antivirus e antimalware installati e aggiornati periodicamente;
- Aggiornamento costante dei software; Firewall con aggiornamento periodico;
- Filtro anti-spam; controllo accessi a siti non sicuri; divieto di installare software non autorizzato.

5.2.5 Crittografia

La crittografia avanzata è applicata alle informazioni che transitano dal server (sala CED) alla sala operativa (Polizia Locale). Per il sistema UAS, i file sono trasferiti su volume cifrato AES-256. Per le

fototrappole Ekiller F4, la crittografia AES-256 è applicata nativamente sulla microSD integrata nel dispositivo, garantendo la protezione dei dati anche in caso di furto o smarrimento dell'apparecchio.

5.2.6 Minimizzazione dei dati

Vengono raccolti e conservati unicamente i dati necessari. Le fototrappole Ekiller F4 contribuiscono alla minimizzazione grazie alla funzione Smart Detection, che avvia la registrazione solo in corrispondenza di eventi rilevanti.

5.2.7 Archiviazione e backup

L'archiviazione avviene in conformità alle procedure comunali. Le immagini del sistema VDS non sono oggetto di backup; il backup è presente soltanto sui client delle immagini esportate. Le immagini delle fototrappole sono archiviate sulla microSD crittografata del dispositivo.

5.2.8 Controllo degli accessi fisici

- Accessi fisici limitati e controllati;
- Chiavi dei locali custodite dal solo personale della Polizia Locale;
- Lucchetto porta esterna; server in armadio con serratura;
- Le fototrappole Ekiller F4 sono protette da gabbia in acciaio inox con catena da 2,5 m e 2 lucchetti antifurto.

5.2.9 Sicurezza dell'hardware

- Manutenzione programmata; distruzione supporti non utilizzati;
- Estintori e revisione periodica; porte tagliafuoco;
- Accordo di assistenza continuativa con ditta specializzata;
- Per le fototrappole Ekiller F4: grado di protezione IP66, temperatura operativa -20°C/+50°C, valigia antiurto.

5.2.10 Manutenzione

Manutenzione programmata degli strumenti, manutenzione costante degli impianti, controllo sull'operato degli addetti.

5.2.11 Sicurezza dei canali informatici

- Crittografia nelle comunicazioni server-sala operativa;
- Controlli periodici sulla protezione nella trasmissione dei dati;
- Firewall installato e aggiornato periodicamente.

5.2.12 Politica di tutela della privacy

L'Ente ha predisposto una struttura interna per la gestione della privacy con ruoli, compiti e responsabilità formalizzati. Il trattamento è effettuato solo da soggetti formalmente incaricati. Misure adottate:

- Formazione al momento dell'ingresso in servizio e periodica;
- Formazione specifica per operatori del sistema UAS e per l'utilizzo delle fototrappole Ekiller F4, incluse le procedure di esportazione, crittografia e Digital Watermarking;
- Istruzioni sulla custodia dei documenti, protezione degli strumenti, segretezza delle credenziali;
- Aggiornamento periodico della lista degli incaricati e dei profili di autorizzazione;
- Procedure di verifica e sanzioni disciplinari.

5.2.13 Misure di sicurezza specifiche

Ai sensi dell'art. 24 del GDPR e dell'art. 29, co. 2, della Direttiva (UE) 2016/680, sono adottate misure per: vietare l'accesso non autorizzato alle attrezzature; impedire lettura, copia o modifica non autorizzata; garantire la tracciabilità delle trasmissioni e delle introduzioni; impedire la lettura o copia durante i trasferimenti; garantire il ripristino in caso di interruzione; garantire l'affidabilità e l'integrità dei dati. Il Digital Watermarking delle fototrappole Ekiller F4 fornisce un ulteriore livello di garanzia sull'integrità e sull'autenticità delle registrazioni.

5.3 Accesso illegittimo ai dati

5.3.1 Impatti potenziali

Diffusione non autorizzata delle immagini, intercettazione di informazioni in rete, pregiudizio alla reputazione, possibile discriminazione.

5.3.2 Principali minacce

Abuso di privilegi, accesso non autorizzato, furto nei locali o delle fototrappole, vulnerabilità degli asset, virus informatici, spamming, social engineering.

5.3.3 Fonti di rischio

Fonti interne (personale non autorizzato o negligente) ed esterne (attaccanti informatici, virus, malware). Per le fototrappole: rischio di furto del dispositivo fisico mitigato dalla crittografia AES-256 sulla microSD e dalla protezione fisica (gabbia in acciaio, catena, lucchetti).

5.3.4 Misure di mitigazione

Anonimizzazione; controllo degli accessi logici e tracciabilità; sicurezza dei documenti cartacei; protezione contro malware; crittografia (inclusa AES-256 nativa sulle fototrappole); minimizzazione; controllo degli accessi fisici; manutenzione; sicurezza dei canali informatici; politica di tutela della privacy; misure di sicurezza specifiche; Digital Watermarking.

5.3.5 Valutazione

Gravità: 2 – Limitata. La natura dei dati (immagini di aree pubbliche, targhe) circoscrive l'impatto individuale.

Probabilità: 2 – Limitata. Le misure adottate (circuito chiuso, credenziali personali, crittografia AES-256, accessi fisici controllati) riducono significativamente il rischio.

Rischio residuo: 4 (Basso). Accettabile con le misure adottate.

5.4 Modifiche indesiderate dei dati

5.4.1 Impatti potenziali

Alterazione dei dati, negazione dell'accesso a servizi, pregiudizio alla reputazione.

5.4.2 Principali minacce

Accesso non autorizzato, sottrazione di credenziali, errore umano, comportamenti contrari ai principi di sicurezza.

5.4.3 Fonti di rischio

Utenti interni, soggetti esterni, attacchi informatici.

5.4.4 Misure di mitigazione

Controllo degli accessi logici e tracciabilità; protezione contro malware; crittografia; minimizzazione; archiviazione e backup; controllo accessi fisici; sicurezza dei canali informatici; politica di privacy; misure specifiche. Il Digital Watermarking delle Ekiller F4 consente di verificare l'integrità delle registrazioni e di rilevare eventuali manomissioni.

5.4.5 Valutazione

Gravità: 2 – Limitata. L'alterazione delle immagini ha un impatto contenuto grazie alla natura temporanea dei dati e al Digital Watermarking.

Probabilità: 2 – Limitata. Tracciabilità, credenziali personali e formazione riducono la probabilità.

Rischio residuo: 4 (Basso). Accettabile con le misure adottate.

5.5 Perdita di dati

5.5.1 Impatti potenziali

Indisponibilità dei dati, danno reputazionale, impossibilità di fornire elementi di prova.

5.5.2 Principali minacce

Errori umani, eventi distruttivi, malfunzionamento, guasti, sottrazione di strumenti (incluso furto delle fototrappole), virus informatici.

5.5.3 Fonti di rischio

Utenti interni, soggetti esterni, attacchi informatici, eventi calamitosi, malfunzionamenti.

5.5.4 Misure di mitigazione

Controllo degli accessi logici; protezione contro malware; crittografia; minimizzazione; archiviazione e backup; controllo accessi fisici (incluse gabbia, catena e lucchetti per le fototrappole); sicurezza dell'hardware; sicurezza dei canali informatici; politica di privacy; misure specifiche.

5.5.5 Valutazione

Gravità: 2 – Limitata. La conservazione massima di 7 giorni limita l'impatto temporale.

Probabilità: 2 – Limitata. Le misure di sicurezza fisica e logica riducono la probabilità.

Rischio residuo: 4 (Basso). Accettabile con le misure adottate.

5.6 Riepilogo della valutazione dei rischi

Scenario	Gravità	Probabilità	Rischio	Livello
Accesso illegittimo	2	2	4	**Basso**
Modifiche indesiderate	2	2	4	**Basso**
Perdita di dati	2	2	4	**Basso**

6. Esito della valutazione d'impatto

Alla luce dell'analisi condotta, il trattamento dei dati personali mediante il sistema di videosorveglianza fisso (96 telecamere), le n. 2 fototrappole mobili Ekiller F4, i n. 2 rilevatori di infrazione semaforica Autosc@n RED e il sistema UAS (Drone DJI Air 3S) del Comune di Bassano Romano presenta un livello di rischio residuo complessivamente basso per i diritti e le libertà degli interessati.

Le misure tecniche e organizzative adottate e pianificate – tra cui il sistema a circuito chiuso, la crittografia AES-256 (sia sulle fototrappole sia sul volume UAS), il Digital Watermarking, il controllo degli accessi logici e fisici, la formazione del personale, la conservazione limitata dei dati e la tracciabilità degli accessi – risultano adeguate a mitigare i rischi individuati.

Consultazione preventiva. Ai sensi dell'art. 36 del GDPR, non si ritiene necessario procedere alla consultazione preventiva del Garante, in quanto le misure adottate sono sufficienti a ridurre il rischio residuo a un livello accettabile.

Piano d'azione. Si raccomandano le seguenti azioni di miglioramento continuo:

- verifica annuale dell'adeguatezza delle misure di sicurezza e aggiornamento della presente DPIA;
- formazione periodica del personale autorizzato, con sessioni specifiche per operatori UAS e per l'utilizzo delle fototrappole Ekiller F4;
- audit periodici sugli accessi logici e sulle procedure di conservazione e cancellazione;
- aggiornamento del Registro dei trattamenti in caso di modifiche al sistema;
- verifica della conformità alla normativa ENAC/EASA per l'impiego del drone;
- inventario periodico delle fototrappole con verifica dell'integrità fisica e funzionale dei dispositivi.

7. Parere del Responsabile della Protezione dei Dati (DPO)

Ai sensi dell'art. 35, par. 2, del GDPR, il Titolare del trattamento ha consultato il DPO nell'ambito della presente valutazione d'impatto.

Il DPO, esaminata la documentazione relativa al trattamento, le misure di sicurezza adottate e pianificate, e la valutazione dei rischi effettuata, esprime il seguente parere:

[Inserire il parere del DPO, comprensivo di eventuali osservazioni, raccomandazioni e conclusioni sulla conformità del trattamento al GDPR e alla normativa applicabile.]

Data: _____ Il DPO _____ (Nome, Cognome e Firma)	Data: _____ Il Titolare del trattamento _____ (Il Sindaco)

Allegato 1 – Informazioni tecniche sul sistema di videosorveglianza

A. Impianto di videosorveglianza fisso

N. telecamere	Finalità di utilizzo	Luogo di installazione
96	Tutela della sicurezza urbana e pubblica; Tutela del patrimonio comunale; Tutela ambientale e polizia amministrativa; Tutela della sicurezza stradale e controllo circolazione (lettura targhe).	*Vedasi tabella seguente*

Elenco dei punti di installazione

N.	Ubicazione
1	Piazzale Gramsci
2	Scalette di via Serapina
3	Via San Vincenzo incrocio con via Sant'Andrea (Monastero)
4	Via San Vincenzo incrocio con via Sant'Andrea (Centro)
5	Parcheggio Fonte Vignale (lavatoio)
6	Parcheggio Fonte Vignale (parcheggio)
7	Via San Vincenzo dalla Chiesa di San Gratiliano verso Monastero
8	Largo Donatori di Sangue (IV Novembre)
9	Largo Donatori di Sangue (San Gratiliano)
10	Largo Giuseppe Altobelli (Fratelli Bandiera)
11	Largo Giuseppe Altobelli (Largo Cairoli)
12	Via della Stazione – Isola Ecologica (ingresso)
13	Via della Stazione – Isola Ecologica (OCR ingresso)
14	Via della Stazione – Isola Ecologica (interno)
15	Piazza Umberto I° (piazza/via Roma)
16	Piazza Umberto I° (Municipio)
17	Via Maria Giustiniani
18	Via della Stazione inc. S.P. 40 (normale)
19	Via della Stazione inc. S.P. 40 (OCR)
20	Via IV Novembre (Parco Mario Cenciarini)
21	Parcheggio San Gratiliano (ingressi)
22	Via San Gratiliano fronte civ. 31 (centro storico)
23	Via San Gratiliano fronte civ. 31 (Largo San Gratiliano)
24	Via della Stazione loc. Galilea (campo polifunzionale)
25	Via della Stazione impianti sportivi (parcheggio)
26	Via Giuseppe Mazzini (Largo Mazzini)

27	Via della Stazione (Palazzetto dello Sport)
28	Via Leonardo da Vinci inc. via Montecastello
29	Via Leonardo da Vinci inc. via Michelangelo
30	Via Leonardo da Vinci inc. via Santa Lucia (Cassia)
31	Via Leonardo da Vinci inc. via Santa Lucia (Centro)
32	S.P. 40 inc. via Roma (OCR Cassia)
33	Via Roma inc. via Fratelli Bandiera (OCR Zona Artigianale)
34	Via Amerigo Vespucci
35	Via della Stazione inc. via San Pietro (OCR)
36	Via della Stazione inc. via San Pietro (normale)
37	Via Michelangelo B. inc. via B. Cellini
38	Parco Pubblico Mario Cenciarini

B. Fototrappole mobili

Caratteristica	Dettaglio
Modello	Ekiller F4
Quantità	n. 2
Sensore	STARLIGHT 1/2.8″ 2MP CMOS
Risoluzione	FullHD 1080p (1920x1080) a 25 fps
Codifica video	H.265+ e H.264+ Triple-Stream Encoding
Ottiche	Intercambiabili: 2,8 mm / 8 mm / 12 mm / 16 mm / 25 mm
Crittografia	AES-256 su microSD da 256 GB
Digital Watermarking	Sì – garanzia di autenticità e non alterazione
Smart Detection	Oggetto abbandonato/rimosso, intrusione, attraversamento linea, motion detection
Gestione remota	Software VMS Ekiller (PC) e App Mobile in tempo reale
Autonomia batteria	120 ore (estendibile con pacchi aggiuntivi)
Protezione	IP66; temperatura operativa -20°C / +50°C
Dimensioni	≤ 26x23x11 cm; peso max 5.490 g
Protezione fisica	Gabbia in acciaio inox, catena 2,5 m, 2 lucchetti
Registrazione audio	Non presente
Conformità GDPR	Dichiarata dal produttore
Finalità	Contrasto abbandono rifiuti, atti vandalici, polizia giudiziaria, tutela ambientale
Installazione	Mobile/riposizionabile, a terra o a palo, nei siti di interesse operativo

C. Sistema UAS (Drone)

Caratteristica	Dettaglio
Modello	DJI Air 3S

Quantità	n. 1
Registrazione audio	Non presente
Riconoscimento facciale	Non presente
Crittografia	AES-256 su volume dedicato (BitLocker/VeraCrypt)
Finalità	P.G., polizia stradale, sicurezza urbana, documentazione eventi, illeciti edilizi/ambientali, protezione civile, safety eventi

D. Rilevatori di infrazione semaforica (Autosc@n RED)

Caratteristica	Dettaglio
Sistema	Autosc@n RED – Gruppo Maggioli
Quantità	n. 2
Tipologia	Rilevamento e sanzionamento automatico delle violazioni al semaforo rosso
Acquisizione dati	8 immagini per violazione (di cui 2 OCR) + 1 video
Mascheramento privacy	Sì – offuscamento automatico dei dati sensibili nella scena fotografica
Ricerca proprietario	Integrazione con banca dati DTTSIS (motorizzazione)
Software gestionale	Piattaforma Autosc@n con interfaccia nativa Concilia Software
Modalità di erogazione	Cloud – Data center Gruppo Maggioli (Italia), qualificato ACN
Responsabile trattamento	Gruppo Maggioli / Concilia Service – nominato ex art. 28 GDPR
Statistiche	Produzione statistiche su transiti e violazioni
Ubicazione dispositivo 1	[INSERIRE INTERSEZIONE SEMAFORICA N. 1]
Ubicazione dispositivo 2	[INSERIRE INTERSEZIONE SEMAFORICA N. 2]
Finalità	Tutela della sicurezza stradale, rilevamento infrazioni art. 146 C.d.S. (passaggio con il rosso), prevenzione incidentalità