Regolamento Comunale per la disciplina e l'utilizzo dei sistemi di videosorveglianza

(approvato con delibera di Consiglio Comunale n 50 del 28.11.2025)

Art.1) Oggetto

1) Il presente regolamento disciplina il trattamento dei dati personali acquisiti mediante l'utilizzo dei sistemi di videosorveglianza attivati nel territorio del Comune di Gossolengo, determinandone le condizioni necessarie per la tenuta in esercizio, in osservanza delle seguenti disposizioni normative
   - Regolamento UE 2016/679, (GDPR - General Data Protection Regulation);
   - Provvedimento generale in materia di videosorveglianza del Garante per la protezione dei dati personali del 8 aprile 2010 (fatto salvo dall'art.22, comma 4 del D.Lgs.101/2018);
   - Linee guida EDPB 3/2019 sul trattamento dei dati personali attarverso dispositivi video;
   - FAQ di recepimento dell'Autorità Garante (Dicembre 2020).

2) L'applicazione della suddetta disciplina normativa si rende necessaria in quanto i sistemi di videosorveglianza rilevano e registrano immagini che possono permettere di identificare (in via diretta o indiretta) le persone fisiche riprese o altri elementi ad esse riconducibili, rappresentando di fatto "dati personali", ai sensi della definzione di cui all'Art. 4 del GDPR.

3) L'installazione e l'attivazione dei sistemi di videosorveglianza non deve essere sottoposta all'esame preventivo del Garante, ma è sufficiente che il trattamento dei dati personali effettuato tramite tale tipo di impianto per lo svolgimento dei propri compiti istituzionali avvenga nel rispetto dei requisiti previsti dal GDPR e previa informativa alle persone che stanno per accedere nell'area videosorvegliata.

4) In particolare, il presente regolamento disciplina gli adempimenti, le garanzie e le tutele per il legittimo e pertinente trattamento dei dati personali acquisiti mediante l'utilizzo dei sistemi di videosorveglianza Comunali.

5) Il Comune di Gossolengo si riserva la facoltà di integrare le linee di indirzzo espresse nel presente regolamento con eventuali allegati tecnici in cui dettagliare caratterisitiche tecniche specifiche dei sistemi.

Art.2) Definizioni

Ai fini del presente regolamento si intende:

a) per "Regolamento UE", il Regolamento Ue 2016/679, (GDPR - General Data Protection Regulation) e successive modificazioni ed integrazioni;

b) per "Decreto Legislativo 10 agosto 2018, n. 101" Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

c) per "sistemi di videosorveglianza", qualunque impianto di ripresa, fissa o mobile, composto da una o più telecamere (o dispositivo di acquisizione immagini assimilabile, a titolo esemplificativo fototrappole, bodycam, ecc.), in grado di riprendere e registrare immagini e suoni, utilizzato per le finalità indicate dall'articolo 3 del presente regolamento;

d) per "banca di dati", il complesso di dati personali che, in relazione ai luoghi di installazione delle videocamere, riguardano i soggetti che transitano nell'area interessata, anche archiviati all'interno di Video Server / memorie digitali dedicati, e trattati esclusivamente da un ristretto numero di soggetti appositamente designati ed incaricati per iscritto;

e) per "trattamento", tutte le operazioni o complesso di operazioni, svolte con l'ausilio dei mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la selezione, l'estrazione, l'utilizzo, l'interconnessione, la comunicazione, l'eventuale diffusione, la cancellazione e la distribuzione di dati;

f) per "dato personale", qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, e rilevata con trattamenti di immagini effettuati attraverso l'impianto di videosorveglianza;

g) per "misure di sicurezza", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che garantiscono il livello adeguato di protezione previsto dalle norme (GDPR, Art.32);

h) per "titolare", il Comune di Gossolengo, in persona del Sindaco pro-tempore, al quale compete il potere decisionale autonomo in ordine alle finalità ed alle modalità del trattamento dei dati personali;

i) per "responsabile esterno", la persona fisica/giuridica, legata da rapporto di servizio al titolare e preposto al trattamento dei dati personali;

j) per "autorizzato", la persona fisica autorizzata ed istruita a compiere operazioni di trattamento dal titolare o dal responsabile;

k) per "interessato", la persona fisica cui si riferiscono i dati personali (soggetti ripresi);

l) per "Garante", il garante per la protezione dei dati personali;

m) per "Privacy by default e Privacy by Design" i principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita sanciti dall'Art.25 del GDPR;

n) per "Data Breach" la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

o) per "Data Protection Officer" il responsabile della protezione dei dati, come definito dagli Artt.37-39 del GDPR;

p) per "Analisi dei rischi" la valutazione dei rischi presentati dal trattamento (in termini di gravità e probabilità) che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Art.3) Finalità

1) Le finalità di utilizzo dei sistemi di videosorveglianza di cui al presente regolamento sono conformi alle funzioni istituzionali demandate ai Sindaci ed ai Comuni dal decreto legge n. 14 del 20 febbraio 2017 convertito in legge n. 48 del 13 aprile 2017 "disposizioni urgenti in materia di sicurezza delle città", dallo statuto e dai regolamenti comunali e dalle altre disposizioni normative applicabili al Comune di Gossolengo. In particolare, l'uso di impianti di videosorveglianza è strumento per l'attuazione di un sistema integrato di politiche per la sicurezza urbana, di cui alle fonti normative sopra citate.

2) L'utilizzo degli impianti di videosorveglianza è finalizzato a:
   - prevenire e reprimere atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" di cui all'articolo 4 del decreto legge n. 14/2017 e delle attribuzioni del Sindaco in qualità di autorità locale di cui all'art. 50 e di ufficiale di governo di cui all'art. 54 comma 4 e 4-bis del d.lvo 267/2000;
   - prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado e abbandono di rifiuti, e svolgere i controlli volti ad accertare e sanzionare le violazioni delle norme contenute nel regolamento di polizia urbana, nei regolamenti locali in genere e nelle ordinanze sindacali;
   - vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato,
   - tutelare l'ordine, il decoro e la quiete pubblica;
   - controllare aree specifiche del territorio comunale, particolarmente esposte a rischi di sicurezza;
   - monitorare i flussi di traffico ed eventuali violazioni del codice della strada o di altre disposizioni normative, quali obblighi di assicurazione o revisione veicoli.

3) Ai sensi di quanto previsto dall'articolo 4 della Legge 20 maggio 1970, n. 300 e dal Regolamento Ue 2016/679 (GDPR) e successive integrazioni e modifiche, gli impianti di videosorveglianza non possono essere utilizzati per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

Art.4) Principi applicabili al trattamento dei dati personali

1) Il presente regolamento garantisce che il trattamento dei dati personali, acquisiti mediante l'utilizzo degli impianti di videosorveglianza gestiti dal Comune di Gossolengo si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

2) L'utilizzo degli impianti di videosorveglianza comporta esclusivamente il trattamento di dati personali rilevati mediante le riprese video che, in relazione ai luoghi di installazione delle telecamere, interessano i soggetti, o altri elementi ad essi ricondubili, che transitano nell'area oggetto di sorveglianza.

3) Il trattamento dei dati personali si svolge nel pieno rispetto dei principi di liceità, finalità, necessità e proporzionalità, sanciti dal GDPR.

4) In attuazione dei principi di **liceità** e **finalità**, il trattamento dei dati personali acquisiti mediante l'utilizzo dei sistemi di videosorveglianza è effettuato dal Comune di Gossolengo esclusivamente per lo svolgimento delle funzioni istituzionali e per il perseguimento delle finalità di cui all'articolo 3 del presente regolamento.

5) In attuazione del principio di **necessità**, i sistemi di videosorveglianza ed i programmi informatici di gestione sono configurati in modo da ridurre al minimo l'uso di dati personali ed identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere raggiunte mediante dati anonimi o con modalità che permettano di identificare l'interessato solo in caso di necessità.

6) In attuazione del principio di **proporzionalità** e dei criteri di pertinenza e non eccedenza, i sistemi di videosorveglianza sono configurati in modo da raccogliere esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese ed evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti.

Art.5) Titolare e Responsabile della protezione dei dati

1) Il Comune di Gossolengo è Titolare del trattamento dei dati personali acquisiti mediante utilizzo degli impianti di videosorveglianza di cui al presente regolamento. A tal fine il Comune di Gossolengo è rappresentato dal Sindaco, a cui compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza. Il sistema di videosorveglianza è registrato presso un server ubicato in Rivergaro – Strada Provinciale per Gossolengo n. 6/D, presso il Comando dell'Associazione Intercomunale "Bassa Valtrebbia" in virtù della Convenzione sottoscritta in data 27 febbraio 2025.

2) Il sistema di telecamere può essere condiviso tra autonomi Titolari del trattamento che perseguono propri compiti istituzionali ai fini e per gli effetti del paragrafo 4.6 del "Provvedimento in materia di Videosorveglianza dell'08 aprile 2010 (Sistemi integrati di Videosorveglianza).

3) L'Ente Comune, in persona del Sindaco pro-tempore, la Compagnia Carabinieri Nucleo Operativo e Radiomobile di Bobbio, in persona del Comandante pro tempore, e il Comando della Stazione dei Carabinieri di Rivergaro, in persona del Comandante pro tempore detengono la titolarità autonoma del trattamento dei dati personali acquisiti mediante utilizzo degli impianti di videosorveglianza – **con riguardo alla sola lettura targhe** - di cui al presente regolamento. Essi determinano in modo trasparente, **mediante un'apposita convenzione**, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente atto; Tale allegato può essere aggiornato senza che ciò comporti una modifica del presente regolamento, attribuendo sin da ora valore cogente a modifiche/aggiornamenti dell'allegato medesimo disposti dal Titolare del trattamento.

   Il Sindaco e/o la Compagnia Carabinieri Nucleo Operativo e Radiomobile di Bobbio, in persona del Comandante pro tempore, e il Comando della Stazione dei Carabinieri di Rivergaro, in persona del Comandante pro tempore, in qualità di rappresentanti dei titolari autonomi del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza, perseguono le proprie finalità istituzionali, delle quali rispondono nelle sedi competenti.

4) I Titolari autonomi ottemperano, ai seguenti obblighi:
   a) definiscono le linee organizzative per l'applicazione della normativa di settore;
   b) nominano i soggetti coinvolti nella gestione del sistema di videosorveglianza, impartendo istruzioni ed assegnando compiti e responsabilità;
   c) dettano le linee guida di carattere fisico, logico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza;
   d) vigilano sulla puntuale osservanza delle disposizioni impartite.

Il Comune di Gossolengo si riserva, in fututro, di stipulare un accordo per l'accesso diretto alle immagini delle telecamere di sua proprietà a tutte le Forze di Polizia del territorio provinciale, previa richiesta di parere al Comitato Provinciale per l'Ordine e la Sicurezza Pubblica.

5) Il Titolare del trattamento si avvale della collaborazione del Responsabile della protezione dei dati, il quale, come per le ulteriori attività di trattamento effettuate dal Comune, è chiamato, ai sensi dell'Art.39 del GDPR, a:
   - informare e fornire consulenza in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
   - sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
   - fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
   - cooperare con l'autorità di controllo; e
   - fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Art.6) Responsabili esterni del trattamento dei dati personali

1) Il Titolare è chiamato a nominare Responsabili del trattamento dei dati personali acquisiti mediante l'utilizzo dei sistemi di videosorveglianza, in conformità alle indicazioni dell'Art.28 del GDPR, i soggetti esterni di cui potrebbe avvalersi per attività connesse ad installazione, configurazione, manutenzione, assistenza, ampliamento del sistema, nonché per attività e servizi di vigilanza. Nel provvedimento di nomina sono analiticamente specificati i compiti affidati al responsabile.

2) I responsabili effettuano il trattamento nel rispetto della normativa vigente in materia di protezione dei dati personali, ivi incluso il profilo della sicurezza, e delle disposizioni del presente regolamento.

Art.7) Persone autorizzate al trattamento dei dati personali

1) Per la gestione operativa del sistema, il Titolare nomina ed istruisce i soggetti autorizzati al trattamento. Gli autorizzati sono nominati tra il personale del Comune di Gossolengo o enti correlati che per esperienza, capacità e affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati (di norma all'interno dei settori tecnici o di polizia municipale).

2) L'incarico è effettuato con atto scritto, nel quale sono analiticamente specificati i compiti affidati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati. I profili di accesso ed i livelli di autorizzazione possono essere differenziati, in conformità all'Art. 2-quaterdecies del D.Lgs.196/2003, in modo da assegnare correttamente ruoli ed attività.

3) Gli autorizzati sono tenuti a:
   - svolgere le attività previste dall'atto di autorizzazione secondo le prescrizioni in esso contenute e le direttive del Titolare/DPO;
   - rispettare le norme di sicurezza per la protezione dei dati personali, astenendosi da qualsiasi utilizzo improprio e non necessario del sistema;
   - informare il Titolare/DPO in caso di incidente di sicurezza che coinvolga l'impianto;
   - informare il Titolare/DPO in caso di richiesta di accesso alle registrazioni da parte di soggetti interessati o autorità giudiziaria.

Art.8) Collocamento/orientamento delle telecamere e misure di sicurezza

1) Il cono di ripresa delle telecamere deve essere impostato in modo tale da focalizzare l'obiettivo sul controllo e la registrazione di quanto accada in luoghi pubblici o aperti al pubblico, con particolare attenzione al rispetto del divieto di interferenze illecite nella vita privata (ripresa di private dimore).

2) Eventuali strumenti che consentono uno spostamento arbitrario dell'inquadratura (es: telecamere brandeggiabili, telecamere mobili, body-cam, ecc.) devono essere utilizzate, dai soggetti autorizzati, coerentemente con il suddetto principio, comunque al solo fine del raggiungimento degli scopi di cui all'Art.3 del presente Regolamento.

3) I dati sono protetti da idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. In particolare:
   - i monitor di sistemi di videosorveglianza sono collocati in modo tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate;
   - l'accesso ai sistemi avviene secondo adeguate procedure di autenticazione logica;
   - gli apparati di connessione sfruttano protocolli di trasmissione sicuri;
   - le reti informatiche a cui sono connessi agli apparati di ripresa sono protette tramite strumenti di difesa perimetrale e protezione da malware;
   - i sistemi prevedono la tracciatura dei log di accesso e delle operazioni compiute;
   - gli apparati di registrazione delle immagini (recorder, PC/server, memorie locali, ecc.) sono collocati in locali o in supporti ad accesso sicuro e controllato.

4) Eventuali tecnologie/funzioni avanzate associate ai sistemi di videosorveglianza (a titolo esemplificativo, non esaustivo: sistemi di lettura targhe, sistemi di rilevazione termica, apparati barndeggiabili o removibili, fototrappole, sistemi indossabili, sistemi a bordo veicoli, sistemi di videoanalisi, ecc.) dovranno essere installate, configurati ed utilizzati in conformità alle prescrizioni del presente regolamento, con specifico riferimento a:
- Finalità di utilizzo coerenti agli scopi elencati nell'Art.3
- Rispetto dei prinicpi generali di cui all'Art.4
- Assegnazione di ruoli e responsabilità come da Art.6,7
- Implementazione di adeguate misure di sicurezza tecnicvhe ed organizzative, come da Art.8
- Conservazione ed accesso ai dati come da Art.9
- Eventuali approfondimenti tecnici come da Art.14

5) Resta salva la necessità di condurre una valutazione d'impatto sulla protezione dei dati ed eventuale consultazione preventiva dell'Autorità Garante esclusivamente qualora ricorrano i presupposti di cui agli art.36 e 37 del GDPR.

Art.9) Conservazione dei dati personali ed accesso alle registrazioni

1) I dati personali registrati mediante l'utilizzo dei sistemi di videosorveglianza di cui al presente Regolamento sono conservati per un periodo di tempo non superiore ai 7 giorni, ai fini della tutela della sicurezza urbana. Al termine del periodo di conservazione le immagini registrate vengono cancellate tramite sovrascrittura dai relativi supporti elettronici, informatici o magnetici.

2) La conservazione dei dati personali per un periodo di tempo superiore a quello indicato dal comma 1 del presente articolo è ammessa esclusivamente su specifica richiesta della Autorità Giudiziaria o di Polizia Giudiziaria in relazione ad un'attività investigativa in corso.

3) L'accesso alle registrazioni deve avvenire esclusivamente per una verifica collegata alle finalità di cui al paragrafo 3, che comunque può essere effettuata solo da soggetti espressamente autorizzati, evitando la presenza di persone non autorizzate.

4) Qualora si riscontrassero immagini di fatti concernenti ipotesi di reato o di eventi rilevanti ai fini della pubblica sicurezza, della tutela ambientale o del patrimonio pubblico, l'incaricato o il Responsabile provvederà a darne comunicazione senza ritardo all'Ente, provvedendo, su richiesta tracciata di questo, alla riversazione/conservazione delle immagini su appositi supporti.

5) Alle immagini raccolte ai sensi del presente articolo possono accedere, per l'espletamento delle relative indagini, gli appartenenti all'Amministrazione Giudiziaria, le persone da essi espressamente autorizzate e gli organi di Polizia. Qualora gli organi di Polizia, nello svolgimento dei loro compiti istituzionali, necessitino una copia delle riprese effettuate, devono presentare un'istanza scritta e motivata.

6) Il sistema potrà essere interfacciato, per un migliore perseguimento delle finalità di sicurezza istituzionali, ad altri sistemi / banche dati nazionali o locali, già in uso per finalità di prevenzione, accertamento e repressione reati.

Art.10) Informativa

1) L'informazione sulla presenza di impianti di videosorveglianza cittadini è assicurata mediante appositi cartelli segnaletici conformi alle prescrizioni dell'Autorità Garante, collocati in modo chiaramente visibile nelle aree cittadine video sorvegliate.

2) Il supporto con l'informativa:
   - deve essere collocato nei luoghi ripresi o nelle immediate vicinanze, non necessariamente a contatto con la telecamera, possibilmente in modo da riusltare visibile in prossimità dell'accesso all'area videosorvegliata;
   - deve avere un formato ed un posizionamento tale da essere chiaramente visibile.

3) Il Comune provvederà inoltre a pubblicare sul proprio sito internet istituzionale un'informativa circostanziata contenente tutti gli elementi previsti dall'Art.13 del GDPR.

Art.11) Cessazione del trattamento dei dati personali

1) In caso di cessazione, per qualsiasi causa, del trattamento, i dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento verranno distrutti.

Art.12) Diritti dell'interessato

1) È assicurata agli interessati la facoltà di esercitare, per quanto compatibile con i trattamenti connessi al sistema di videosorveglianza, i diritti di cui agli Art.15-21 del GDPR: diritto di accesso, rettifica, cancellazione, limitazione, portabilità, opposizione.

2) L'interessato potrà in qualsiasi momento esercitare i suddetti diritti inviando una mail al Titolare o al Data Protection Officer ai recapiti indicati sul sisto internet istituzionale dell'Ente. Qualora l'interessato si rivolgesse ai soggetti autorizzati per l'esercizio dei diritti essi saranno tenuti ad inoltrare la richiesta al Titolare o al Data Protection Officer.

3) In caso di mancato riscontro, l'interessato può proporre reclamo anche al Garante della Privacy via posta ordinaria tramite raccomandata A/R (Piazza di Montecitorio 121, 00186 Roma), oppure tramite pec all'indirizzo protocollo@pec.gpdp.it.

4) La risposta ad una richiesta di esercizio dei diritti di cui agli Art.15-21 del GDPR deve riguardare i dati attinenti alla persona istante identificabile e può comprendere eventuali dati riferiti a terzi, solo nei limiti previsti dalla Legge. L'istanza di accesso è diretta e personale, ovvero resa mediante procura speciale a norma di legge.

Art.13) Ulteriori profili di conformità

1) La videosorveglianza, costituendo attività di trattamento di dati personali, rientra nel sistema privacy GDPR complessivo dell'Ente, in conformità al quale sarà gestito:
   - l'inserimento nel registro dei trattamenti (GDPR, Art.30);
   - la valutazione di rischio e di idonee misure di sicurezza (GDPR, Art.32);
   - la coerenza ai requisiti di "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" (Privacy by design e by default, GDPR, Art.25);
   - la gestione di eventuali incidenti di sicurezza che dovessero coinvolgere il sistema (Data breach, GDPR, Art.33,34);
   - la valutazione di eventuali necessità di Valutazioni di Impatto (Data Protection Impact Assessment, GDPR, Art.35).

Art.14) Aggiornamento allegati tecnici

1) Al fine di integrare il presente regolamento con approfondimenti specifici circa la composizione e le modalità di utilizzo dei sistemi di videosorveglianza il Comune di Gossolengo si riserva la facoltà di redigere appositi allegati tencici, ad uso strettamente riservato, riportanti:
   - collocamento ed orientamento telecamere;
   - valutazioni conformità sulle aree riprese;
   - caratteristiche tecniche apparati e misure di sicurezza;
   - ruoli ed attività soggetti coinvolti;
   - fac-simile cartellonistica "Area videosorvegliata";
   - informativa circostanziata;
   - modelli per accesso ed estrazione immagini;

- modelli per nomina soggetti autorizzati e responsabili esterni.

Art.15) Norma di rinvio

1) Per quanto non espressamente disciplinato dal presente Regolamento, si applicano le disposizioni normative nazionali e regionali vigenti in materia e le disposizioni dello Statuto e del Regolamento di funzionamento del Consiglio Comunale e alle disposizioni vigenti in tema di privacy.

Art.16) Entrata in vigore

1) Il presente regolamento entra in vigore decorsi quindici giorni dalla data di pubblicazione all'albo pretorio, fatti salvi i tempi tecnici necessari all'organizzazione del servizio.

2) Le eventuali e successive modifiche al presente regolamento entrano in vigore decorsi quindici giorni dalla data di pubblicazione all'albo pretorio on line, da effettuarsi dopo che la relativa deliberazione di approvazione o determina dirigenziale sia divenuta esecutiva. Lo stesso verrà inserito nella raccolta ufficiale dei Regolamenti comunali.

ALLEGATO TECNICO DI CONFORMITÀ PRIVACY
RELATIVO AL SISTEMA DI VIDEOSORVEGLIANZA COMUNALE

Redatto ai sensi e per gli effetti di:
Regolamento UE 2016/679 "General Data Protection Regulation"
D.Lgs.196/2003 "Codice in materia di protezione dei dati personali"
Provvedimento in materia di videosorveglianza del 08/04/2010
Linee guida videosorveglianza Dicembre 2020

Ad integrazione di:
Regolamento Comunale per la gestione del sistema di videosorveglianza

Sviluppato e coordinato con:
Linee guida ANCI per i Comuni in materia di Videosorveglianza

INDICE

1) SCOPO DEL DOCUMENTO

Il presente documento è finalizzato ad integrare il Regolamento Comunale sulla Videosorveglianza, con evidenze specifiche sui **profili di conformità operativi e tecnici** alle vigenti normative in materia di privacy del sistema di videosorveglianza in capo al Comune di Gossolengo, fornendo:

• un'evidenza di **profili normativi** rispetto ai quali si sono definite le configurazioni e le modalità di utilizzo del sistema	▶ **CAPITOLO 2**
• una descrizione dei principali **profili tecnici** del sistema (caratteristiche tecniche apparati, collocamento ed orientamento telecamere)	▶ **CAPITOLO 3**
• una classificazione dei **requisiti di conformità** normativa (principi generali, ruoli e responsabilità, misure di sicurezza, informative)	▶ **CAPITOLO 4**
• un elenco delle **procedure tecniche e modulistica** per il corretto utilizzo del sistema (procedure di accesso ed estrazione immagini dal sistema; procedura di risposta a richieste di diritti degli interessati; procedura per gestione incidenti di sicurezza – data breach)	▶ **CAPITOLO 5**

2) NORMATIVE E STANDARD DI RIFERIMENTO

2.1) Premesse normative e provvedimenti di riferimento in materia di videosorveglianza

L'adozione di sistemi di videosorveglianza è in crescita costante. Questi sistemi trattano dati personali come l'immagine che sono da considerarsi, in base alla Direttiva 95/46/CE ed alla normativa italiana, **informazioni riferite ad una persona identificata o identificabile**. Le dimensioni assunte dal fenomeno, soprattutto grazie alle possibilità offerte dalle nuove tecnologie, hanno spinto il Garante ad intervenire per individuare un punto di equilibrio tra esigenze di sicurezza, prevenzione e repressione dei reati, e diritto alla riservatezza e libertà delle persone. Nel luglio del 2000 è stata portata a termine la prima indagine sulla presenza di telecamere visibili in Italia. Nel novembre 2000 il Garante ha emanato delle linee guida contenenti gli indirizzi per garantire che l'installazione di dispositivi per la videosorveglianza rispetti le norme sulla privacy e sulla tutela della libertà delle persone, in particolare assicurando la proporzionalità tra mezzi impiegati e fini perseguiti. La materia è stata poi ulteriormente regolata da due **provvedimenti generali del Garante**, emanati rispettivamente nel 2004 e nel 2010, che contengono prescrizioni vincolanti per tutti i soggetti che intendono avvalersi di sistemi di videosorveglianza e precise garanzie per la privacy dei soggetti i cui dati vengano eventualmente raccolti e trattati tramite tali sistemi. Il provvedimento del 2010, in particolare, sostituisce il precedente e lo integra tenendo conto delle più recenti disposizioni normative in materia e delle possibilità offerte dalle nuove tecnologie.

Di seguito si riportano, oltre ai provvedimenti generali, le decisioni più significative dell'Autorità riguardanti il settore, gli articoli della Newsletter, i comunicati stampa e altre notizie sull'argomento, utili a contestualizzare il panorama normativo di riferimento della presente relazione. Ogni provvedimento di seguito citato è consultabile attraverso l'apposita scheda informativa, pubblicata sul sito dell'Autorità Garante al seguente link: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1002987

Provvedimenti principali
Provvedimento in materia di videosorveglianza - 8 aprile 2010 [doc. web. n. 1712680];
Videosorveglianza - Provvedimento generale sulla videosorveglianza - 29 aprile 2004 [doc. web n. 1003482];
Video surveillance - The general provision adopted by the Garante english version [doc. web. 1116810];
Videosorveglianza - Il decalogo delle regole per non violare la privacy - 29 novembre 2000 [doc. web n. 31019];
Parere 4/2004 del Gruppo di lavoro dei Garanti UE per la tutela dei dati personali;
Le linee guida del Consiglio d'Europa sulla videosorveglianza 2002;

Indagine esplorativa
La videosorveglianza esterna visibile: una panoramica su quattro città - Giugno 2000 (13,6 Mb.)

Comunicati stampa
9 novembre 2010 - Videosorveglianza: pronte le regole per i Comuni
27 aprile 2010 - Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy
25 settembre 2008 - Videosorveglianza: ispezioni del Garante privacy in tutta Italia
4 maggio 2005 - Biglietti numerati e videosorveglianza negli stadi. Il parere del Garante
20 maggio 2004 - Videosorveglianza: individuate le nuove garanzie per i cittadini
23 febbraio 2001 - I primi esiti delle ispezioni del Garante mettono in luce diffuse illegalità
5 marzo 2000 - Videosorveglianza: i Comuni devono adeguare alla privacy la ripresa delle immagini
2 aprile 1999 - Video camere anticrimine sugli autobus e alle fermate: come renderle compatibili con la privacy
8 marzo 1999 - Privacy e videosorveglianza
20 gennaio 1999 - Telecamere negli ospedali nel rispetto della privacy

Newsletter
22 settembre 2009 - Telecamere e dati biometrici sotto la lente del Garante
19 maggio 2009 - Videosorveglianza ed esigenze di sicurezza
3 aprile 2009 - Videosorveglianza: no al controllo dei lavoratori
2 marzo 2009 - Vietate le telecamere negli spogliatoi
16 gennaio 2009 - Telecamere con le orecchie: stop del Garante
2 - 8 maggio 2005 - Biglietti numerati e videosorveglianza negli stadi. Il parere del Garante
21 – 27 febbraio 2005 - Videosorveglianza: nuovi interventi del Garante
31 gennaio - 6 febbraio 2005 - Controlli sulle telecamere
22 - 28 novembre 2004 - Familiari spiati nelle camere ardenti. Interviene il Garante
7 - 13 giugno 2004 - Webcam al porto, vietato zoomare
17 - 23 maggio 2004 - Videosorveglianza: nuove garanzie per i cittadini
4 - 10 novembre 2002 - Raffica di sanzioni ad amministrazioni pubbliche
14 - 20 ottobre 2002 - Le linee guida del Consiglio d'Europa sulla videosorveglianza
30 settembre - 6 ottobre 2002 - Videosorveglianza. Il decalogo dei Garanti europei
9 - 15 settembre 2002 - Privacy: telecamere sugli autobus solo se passeggeri garantiti

2.2) Riscontri normativi privacy specifici di riferimento per l'allegato tecnico

Tenuto conto del contesto generale definito nel precedente paragrafo, i requisiti di conformità su cui si basa il funzionamento del sistema di videosorveglianza sono:

- **D.Lgs.196/2003 "Codice in materia di protezione dei dati personali", con specifico riferimento all'Art. 134**

Capo III - Videosorveglianza

Art. 134. Codice di deontologia e di buona condotta
1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini, prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantire la liceità e la correttezza anche in riferimento a quanto previsto dall'articolo 11.

- **Provvedimento in materia di videosorveglianza 08/04/2010 (pubblicato in G.U. N°99 del 29/04/2010)**

Con particolare riferimento ai paragrafi:

Par.2) Trattamento dei dati personali e videosorveglianza: principi generali

Par.3) Adempimenti applicabili a soggetti pubblici e privati
3.1.2. Ulteriori specificazioni: l'informativa eventuale nella videosorveglianza effettuata per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati
3.1.3. Informativa da parte dei soggetti che effettuano collegamenti con le forze di polizia

Par.5) Soggetti pubblici
5.1. Sicurezza urbana
5.2. Deposito dei rifiuti
5.3. Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada
5.4. Ulteriori avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici e, in particolare, da enti territoriali

- **Decreto Legislativo 10 Agosto 2018 N°101, pubblicato in GU N°205 del 04/09/2018**, che ha completato il processo di armonizzazione della vigente normativa italiana in materia di privacy rispetto alle prescrizioni del regolamento europeo, facendo espressamente salvi, tramite l'Art.22, comma4, i provvedimenti dell'Autorità Garante compatibili con il GDPR (tra cui il citato provvedimento generale in materia di videosorveglianza del 08/04/2010).

- **General Data Protection Regulation (GDPR – Reg. UE 2016/679)** Il presente allegato tecnico è sviluppato tenendo conto dei requisiti di conformità previsti dal GDPR, in modo da potersi integrare nel Sistema di Gestione Privacy Comunale.

- **EDPB - Guidelines 3/2019 on processing of personal data through video devices** Linee guida europee, armonizzate con il GDPR, in riferimento al trattamento di dati personali tramite sistemi di videosorveglianza

- **Linee guida dell'Autorità Garante per la Protezione dei Dati personali in materia di videosorveglianza – Dicembre 2020** con cui l'Autorità definisce le corrette modalità attuative di tutti i suddetti riferimenti normativi

2.3) Ulteriori linee guida e riferimenti normativi

Di seguito si forniscono evidenze su ulteriori profili normativi osservati nell'utilizzo del sistema

- **Linee guida ANCI per i Comuni in materia di Videosorveglianza**

Il suddetto Provvedimento generale ha fornito nuove regole in materia di videosorveglianza, aggiornando le disposizioni del 2004, anche alla luce delle nuove competenze attribuite ai Sindaci in tema di sicurezza urbana e per le diverse evoluzioni tecnologiche intervenute negli ultimi anni.

I lavori che hanno portato alla redazione finale del testo del Provvedimento si sono caratterizzati per un proficuo lavoro di collaborazione tra Autorità ed Enti Locali, finalizzato ad esplicitare le novità introdotte e porre l'accento sulla sfera dell'autonomia regolamentare dei Comuni.

E' emersa chiaramente l'importanza che i Comuni si dotino di regole affinché il servizio di videosorveglianza sia sempre più accessibile, trasparente e governato, al proprio interno, attraverso precise responsabilità di gestione.
Sulla base di queste motivazioni si è sviluppato un ulteriore lavoro di collaborazione, che ha generato le suddette "**Linee Guida per i Comuni in materia di Videosorveglianza**", con lo scopo di fornire chiarimenti e strumenti di lavoro per una corretta applicazione, per quanto di competenza dei Comuni, circa l'utilizzo della videosorveglianza, anche ai fini della sicurezza urbana.
LINK: http://www.sicurezzaurbana.anci.it/index.cfm?layout=dettaglio&IdDett=45654

- **Art.615 bis Codice Penale "Interferenze illecite nella vita privata"**

- **Art.4 L.300/70 "Statuto dei lavoratori"**

3) PROFILI TECNICI DEL SISTEMA DI VIDEOSORVEGLIANZA

3.1) Caratteristiche tecniche apparati

Il sistema di videosorveglianza del Comune di Gossolengo è composto dai seguenti apparati tecnici:

- **13 telecamere di contesto**
- **5 telecare lettura targhe**

La visualizzazione delle immagini è possibile sia presso il presidio di Polizia Locale del Comune di Gossolengo, sia presso il Comando dell'Associazione Intercomunale "Bassa Valtrebbia" (istituita con Convenzione sottoscritta in data 27 febbraio 2025) in Rivergaro – Strada Provinciale per Gossolengo n. 6/D ove è ubicato il server del sistema di videosorveglianza.

2		"TELECAMERA BULLET IP 4MPX, LED IR EXIR,4MM Caratteristiche tecniche: "" Sensore 1/3"" progressive scan; "" Risoluzione massima 2688X1520; "" Frame rate 20fps (2688X1520); 25fps (1920X1080); "" Sensibilità 0.01lux@ F1.2 AGC ON, 0 lux con IR; "" D/N ICR; "" Obiettivo 4mm; "" Compressione video H264, MJPEG, H264+; "" Smart futures: Intrusion detection, Line crossing detection; "" Dual stream; "" Portata IR 50mt, EXIR; "" WDR 120dB; "" Alimentazione 12Vdc/POE 7.5W max; "" Temperatura d'esercizio -30°C+60°C, IP66."
1		FORNITURA SWITCH CON CENTRO MANAGED ADATTO ALL'USO ESTERNO PER TELECAMERE E ANTENNA, 5 PORTE 10/100/MANAGED, POE OUTPUT DIMENSIONI 113X139X28MM
1		"CPE - SXT 5 ac Kit Copia di antenne comprensive di staffe a Pipa o palo standard 2 mt. e 2 Box da esterno."

Q.b.		Mano d'opera, **piattaforma 15 mt**, Cavi, tubi di calata, ferramenta, programmazione e quanto necessario per una installazione a regola dell'arte.
24 mesi		Garanzia full service a copertura di tutti gli eventi ordinarie comprensivi di sostituzione apparati se soggetti a guasto per vizio di forma

	VEGA 10	VEGA 11
Software features and Performance		
Lane Detected	1	
Working Distance	Up to 25m - 83 ft	
Detection	>99%	
Reading	up to 98%	
OCR	ANPR (ALPR) engine on board	
Third party OCR	Optional	
Classification	No	Optional
Vehicle Color	No	Optional
Vehicle Marker	No	Optional
Vehicle Model	No	Optional
Video Streaming	No	Color video streaming via standard RTSP protocol
AES256	Yes	
SHA2	Yes	
Compression	JPG	
Configuration		
Web Server	Installation and configuration with on board Web Application	
Integration	REST and binary protocol available	
Date and Hour	Synchronization via NTP protocol	
Software Update	Upgrading via Web Application and integration protocols	
Data Transmission		
FTP	FTP Client mode for remote data transmission	
Standard protocols	REST and binary protocol, XML, SNMP, NTCIP, Customizable message format	
Configuration	Configurable events/actions and metadata	
Wiegand	Optional	
Serial Port	Insulated RS485 / RS422	
Operating Mode		
Free Run	Self triggering based on image analysis, even without plates	
Trigger mode	Image capture and processing triggered by Ethernet or digital signal	

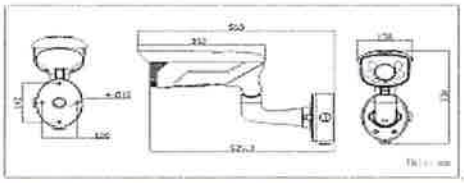
	VEGA 10	VEGA 11
System		
ANPR (ALPR) camera	2 Megapixels Grayscale	
Context camera	No	2 Megapixels Color
Illuminator	8 high power LEDs, InfraRed @ 850 nm	
Lenses	Fixed lens configuration	
Operating System	Linux Operating System	
Custom software	No	Optional
Digital i/o	2 Optoisolated input - 2 Relay Output – 1 Strobe output	
IP Protection	IP68	
Ethernet	GigaBit Ethernet 10/100/1000	
Storage	uSD up to 128 GB	
Vandal proof Connector	Yes	
Antitamper sensor	Yes	
Internal SSD	No	
GPS	No	
LTE	No	
WiFi	Optional	
Technical Data		
Operating & Storage Temperature	From -40° to +60° C - *From -40° to +140° F*	
Operating & Storage Humidity	Up to 95% non condensing	
Dimensions	225 x 132 x 244 mm - *8.85 x 5.2 x 9.6 in (WxHxL)*	
Weight	3,6 kg - 8 lbs	
Power supply voltage	24 Vdc, PoE+	
Power consumption	25W	

Part Numbers

Vega 10-11	
F02010-000	Vega 10
F02011-000	Vega 11

Image Sensor	1/2.8" Progressive Scan CMOS
Min. Illumination	0.005 Lux @(F1.2,AGC ON), 0.007 Lux @(F1.4,AGC ON), 0 Lux with IR
Shutter Speed	1s ~ 1/100,000s
Slow Shutter	Support
Lens	2.8-12mm @ F1.4, angle of view: 105°~32°, 8-32mm @ F1.4, angle of view: 29.7°~9.7°
Auto-iris	DC drive
Day & Night	IR cut filter with auto switch
WDR	120dB
Compression Standard	
Video Compression	H.264+/H.264/ MJPEG
H.264 Type	Baseline Profile / Main Profile / High Profile
Video Bit Rate	32 Kbps ~ 16 Mbps
Audio Compression(-S)	G.711/G.722.1/G.726/MP2L2
Audio Bit Rate(-S)	64Kbps(G.711) / 16Kbps(G.722.1) / 16Kbps(G.726) / 32-128Kbps(MP2L2)
Image	
Max. Resolution	2048×1536
Frame Rate	50Hz: 45fps(2048 × 1536), 50fps@(1920 × 1080, 1280 × 720) 60Hz: 45fps(2048 × 1536), 60fps@(1920 × 1080, 1280 × 720)
Third Stream	Independent with Main Stream and Sub Stream, up to 50/60Hz: 10fps@1280 ×720
Image	BLC/3D DNR/ROI/Defog
Image Setting	Saturation, Brightness, Contrast, Sharpness adjustable by client software or web browser
Regional Cropping	Support
Day/Night Switch	Auto/Schedule/Triggered by Alarm In
Picture Overlay	LOGO picture can be overlaid on video with 128x128 24bit bmp format
Network	
Network Storage	NAS (Support NFS,SMB/CIFS), ANR
Alarm Trigger	Motion detection, Tampering alarm, Network disconnect, IP address conflict, Storage exception
Protocols	TCP/IP, UDP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPnP, SMTP, SNMP, IGMP, 802.1X, QoS, IPv6, Bonjour
Security	User Authentication, Watermark, IP address filtering, Anonymous access
Standard	ONVIF(PROFILE S,PROFILE G),ISAPI
Interface	
Audio (-S)	1-ch 3.5 mm audio in (Mic in/Line in)/out interface
Communication Interface	1 RJ45 10M/100M/1000M Ethernet port, 1 RS-485 interface
Alarm (-S)	1 input, 1 output (up to DC24V 1A or AC110V 500mA)
On-board storage	Built-in Micro SD/SDHC/SDXC slot, up to 128 GB
Reset Button	Yes

Dimensions



Audio (-S)	
Environment Noise Filtering	Support
Audio I/O	Support
Audio Sampling Rate	16kHz / 32kHz / 44.1kHz / 48kHz
Smart Feature-set	
Behavior Analysis	Line crossing detection, Intrusion detection, Region entrance, Region exiting, Unattended baggage, Object removal
Line Crossing Detection	Cross a pre-defined virtual line
Intrusion Detection	Enter and loiter in a pre-defined virtual region
Region Entrance	Enter a pre-defined virtual region from the outside place
Region Exiting	Exit from a pre-defined virtual region
Unattended Baggage	Objects left over in the pre-defined region such as the baggage, purse, dangerous materials
Object Removal	Objects removed from the pre-defined region, such as the exhibits on display
Exception Detections	Scene change detection, Sudden audio increase/decrease detection, Audio loss detection, Defocus detection
Recognition	Face detection recognition
Statistics	Object Counting (Entrance and Exit object number is accounted and showed on screen in real time)
Heat Map	Support
General	
Protection Level	IP66
Impact Protection	IK10
IR Distance	Up to 50m(2.8-12mm)/120m(8-32mm)
Operating Conditions	-30 °C – 60 °C (-22 °F – 140 °F), Humidity 95% or less (non-condensing). -H: -40 °C – 60 °C
Power Supply	24 V AC ± 10%, PoE (802.3at)
Power Consumption	24W MAX
Dimensions	158×338×560 mm (6.22" ×13.31 " × 22.05")
Weight	6200 g (13.67 lbs)
Order Models	
DS-2CD4635FWD-IZ, DS-2CD4635FWD-IZH, DS-2CD4635FWD-IZS, DS-2CD4635FWD-IZHS	

3.2) Collocamento telecamere

Di seguito si forniscono evidenze sul collocamento / orientamento delle telecamere dislocate sul territorio del Comune di Gossolengo.

- TELECAMERA CONTESTO PER STRADELLO PEDONALE E VIA MAZZINI (CONTESTO)
- TELECAMERA CONTESTO VIA SOPRANI INSTALLAZIONE A PALO (CONTESTO)
- TELECAMERA CONTESTO VIA NINO BIXIO INSTALLAZIONE A PALO (CONTESTO)

- TELECAMERA CONTESTO VIA DE SILVESTRI INSTALLAZIONE A PALO (CONTESTO)
- TELECAMERA CONTESTO VIA DOSSETTI QUARTO (CONTESTO)
- TELECAMERA CONTESTO VIA CALCIATI INSTALLAZIONE A PALO (CONTESTO)
- TELECAMERA CONTESTO VIA SUBACCHI SETTIMA (CONTESTO)
- TELECAMERA CONTESTO VIA DEGLI ALPINI SETTIMA (CONTESTO)
- TELECAMERA CONTESTO VIA DELLA COOPERAZIONE GOSSOLENGO (CONTESTO)
- TELECAMERA CONTESTO PIAZZA ROMA (CONTESTO)
- TELECAMERA CONTESTO SP 28 KEROPETROL (CONTESTO)
- TELECAMERA CONTESTO SS 45 – QUARTO INCROCIO 1 (CONTESTO)
- TELECAMERA CONTESTO SS 45 – QUARTO INCROCIO 2 (CONTESTO)
- TELECAMERA LETTURA TARGHE SS 45 – QUARTO DIREZIONE PIACENZA
- TELECAMERA LETTURA TARGHE SETTIMA – VIA DUOMO
- TELECAMERA LETTURA TARGHE VIA MARCONI
- TELECAMERA LETTURA TARGHE SP 28 – ROTATORIA PARTITORE
- TELECAMERA LETTURA TARGHE SP 28 - KEROPETROL

LOC. QUARTO

- Via Donatti
- Via Calciati

LOC. SETTIMA

- Via Don Milani

- Via Subacchi

4) EVIDENZE SUI PROFILI DI CONFORMITA' NORMATIVA

Il presente Capitolo intende fornire evidenze sui profili di conformità previsti dalle vigenti normative in materia di privacy e data protection, con specifico riferimento alle seguenti prescrizioni del GDPR:

PAR.	PROFILO DI CONFORMITA'	RIF.GDPR
4.1	Principi generali di liceità del sistema (privacy by default e privacy by design)	Art.5, 6, 25
4.2	Individuazione attività di trattamento e ruoli dei soggetti coinvolti	Art. 24-29, 30
4.3	Sicurezza del trattamento	Art.32
4.4	Gestione delle violazioni di dati personali	Art.33
4.5	Informativa agli interessati	Art.13
4.6	Diritti degli interessati	Art.15-23

4.1) Principi generali e criteri privacy by design e by default

La normativa prevede alcuni principi generali, dei quali il Titolare del trattamento è responsabile ed in grado di dimostrarne l'applicazione. In particolare è necessario che tutti i dati raccolti dal sistema di videosorveglianza siano:

- *trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);*
- *raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («**limitazione della finalità**»);*
- *adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);*
- *esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»);*
- *conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (**limitazione della conservazione**);*
- *trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («**integrità e riservatezza**»).*

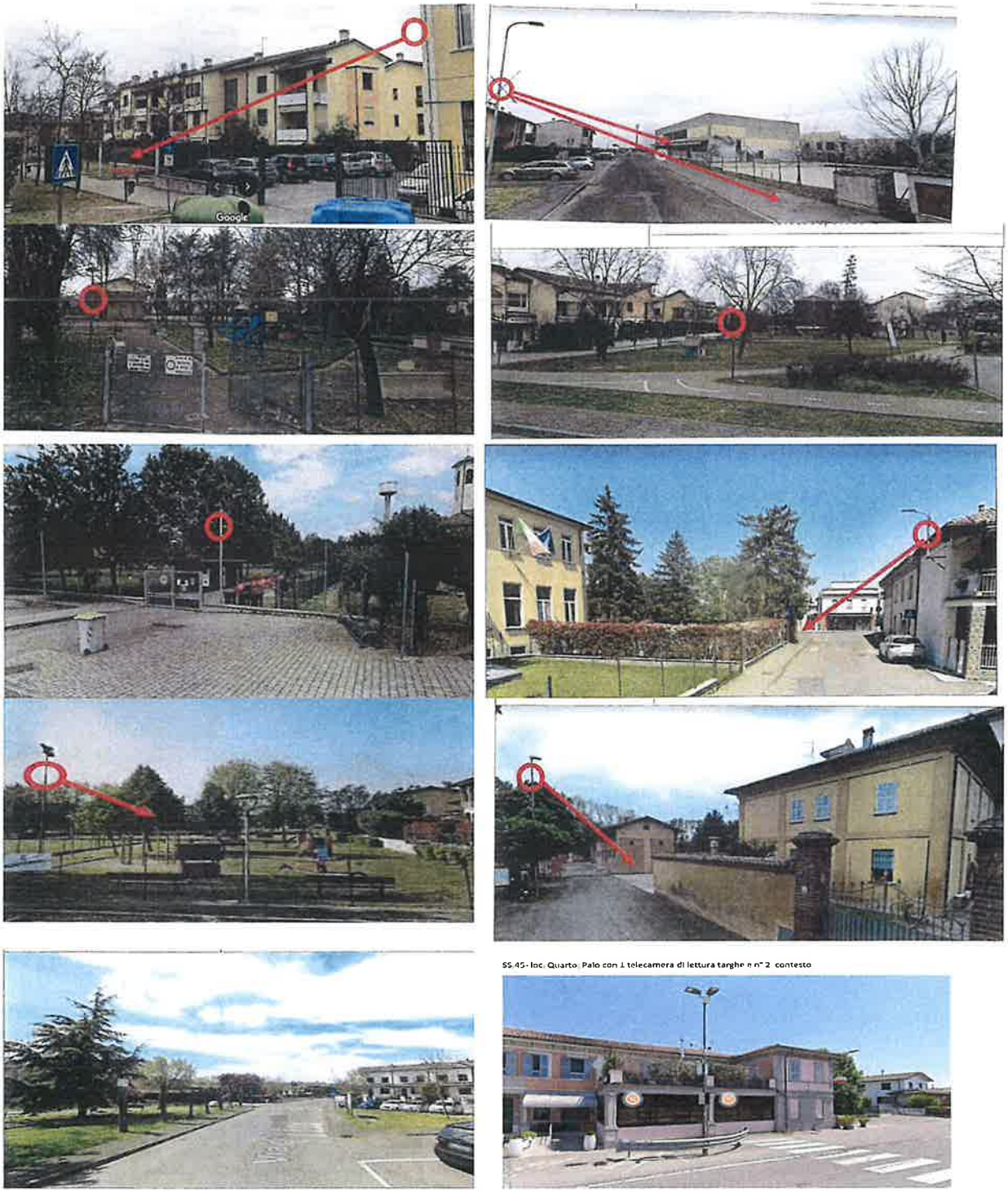
Secondo l'art. 25 del GDPR tali principi devono essere garantiti:

- **fin dalla progettazione** (privacy by design) => collocamento ed orientamento delle telecamere in modo da acquisire solo le immagini necessarie alle finalità del sistema
- **per impostazione predefinita** (privacy by default) => configurazione del sistema in modo da limitare il trattamento e proteggere i dati

Evidenze "Privacy by design"

I seguenti screenshot, estratti dai sistemi, forniscono evidenza del rispetto del principio di privacy by design:

- evidenza di ripresa di aree coerenti con la finalità di ordine e sicurezza pubblica
- evidenza di ripresa di aree non sconfinanti in privata proprietà



Cono di ripresa telecamera di contesto SS.45- Quarto

Cono di ripresa telecamera di contesto SP.28- Gossolengo

SS.45 - via Duomo- Settima: Palo con n° 1 telecamera di lettura targhe

Via Marconi, centro abitato Gossolengo: Palo con n° 1 telecamera di lettura targhe

Strada Agazzana - SP.28- Rotatoria Partitore: n° 1 telecamera lettura targa

cono di ripresa telecamera di contesto

Evidenze "Privacy by default"
La seguente tabella riporta le corrispondenze degli elementi caratterizzanti il criterio di Privacy by default, rispetto ai contenuti del presente documento

CRITERIO PRIVACY BY DEFAULT	CORRISPONDENZA NEL DOCUMENTO
Tempo conservazione	Vedi Par.4.2 (le immagini sono conservate per un periodo massimo di 7 giorni, al termine del quale le più datate vengono automaticamente sovrascritte dalle più recenti)
Cifratura canali di trasmissione	Vedi Par.4.3 ("Misure di sicurezza")
Accesso tramite password	Vedi Par.4.3 ("Misure di sicurezza")
Accesso alle registrazioni solo per specifiche necessità e secondo procedure predefinite	Vedi Capitolo 5

4.2) Soggetti coinvolti ed attività di trattamento

Identificazione Titolare del trattamento, Data Protection Officer e contatti
Il Titolare del Trattamento è lo scrivente Ente, in persona del legale rappresentante pro-tempore (Sindaco):
Comune di Gossolengo
Tel: 0523.770711 – Email: comune.gossolengo@legalmail.it

Il Titolare, ai sensi degli artt. 37-39 del GDPR, ha nominato un Data Protection Officer, al quale è possibile rivolgersi per qualsiasi informazione in materia di privacy o per esercitare i diritti privacy:
ASMEL Associazione
Email: servizio.dpo@asmel.eu – Pec: dpo.asmel@asmepec.it

Identificazione soggetti interni autorizzati all'accesso al sistema
La seguente tabella riporta una classificazione dei **soggetti interni** autorizzati all'utilizzo del sistema, corredata da: cognome/nome; mansione/ufficio; attività autorizzate

Nome/Cognome	Mansione/Settore	Attività autorizzate (descrizione di sintesi)
Paolo COSTA	Comandante	Accesso alle registrazioni; Estrazione di immagini; Visione delle immagini live
Marco DODICI	Agente	Accesso alle registrazioni; Estrazione di immagini; Visione delle immagini live
Stefano CHIESA	Agente	Accesso alle registrazioni; Estrazione di immagini; Visione delle immagini live
Raffaella FERRARONI	Agente	Accesso alle registrazioni; Estrazione di immagini; Visione delle immagini live
Patrizia TAFURI	Agente	Accesso alle registrazioni; Estrazione di immagini; Visione delle immagini live

Identificazione soggetti esterni autorizzati all'accesso al sistema
La seguente tabella riporta una classificazione dei **soggetti a cui viene esternalizzata una o più attività che possono comportare un accesso ai dati**

Ragione sociale /Nome	Ambito di attività esternalizzate
Metronotte Piacenza Srl	Configurazione del sistema; Servizi di assistenza tecnica;
Adyda Srl	Configurazione del sistema; Servizi di assistenza tecnica; Visione delle immagini live

Identificazione della attività di trattamento

Le seguenti tabelle riportano le attività di trattamento connesse al sistema di videosorveglianza, classificando:

- gli elementi del registro dei trattamenti previsti dall'Art.30 del GDPR;
- la valutazione di rischio connessa alle attività, in relazione alla metodologia contenuta in appendice.

ATTIVITÀ' DI TRATTAMENTO	**Nome**	**Visione delle immagini live**		
	Descrizione	Consultazione delle immagini provenienti in live (diretta) dalle telecamere; attività da svolgersi esclusivamente in relazione alle finalità del sistema		
PROFILI DEL TRATTAMENTO	**Categorie di dati**	Immagini videosorveglianza		
	Soggetti interessati	Soggetti ripresi dalle telecamere di videosorveglianza		
	Finalità	Sicurezza e tutela del patrimonio		
	Conservazione	72 ore		
SOGGETTI COINVOLTI	**Autorizzati**	Paolo COSTA; Marco DODICI; Stefano CHIESA; Raffaella FERRARONI; Patrizia TAFURI		
	Destinatari	Trattamento del dato prevalentemente interno (con possibile conoscibilità all'esterno solo per obblighi di legge o contrattuali, di norma senza attività di elaborazione da parte dei soggetti esterni)		
	Responsabili esterni	Adyda Srl		
	Contitolare	n/a		
	Diffusione	Non sono oggetto di diffusione		
	Trasferimenti all'estero	n/a		
	Base del trasferimento	n/a		
STRUMENTI	**Repository**	Utilizzo di strumenti digitali (file, cartelle, database, ecc.) di norma su rete o infrastrutture di back-up interne o collocate in cloud in paesi UE o comunque ritenuti adeguati		
CALCOLO DEL LIVELLO DI RISCHIO E VALUTAZIONI DI IMPATTO	**GRAVITÀ**	2 *(valore assegnato in relazione alla natura del dato)*		
	PROBABILITÀ	1 *(valore assegnato in relazione alla probabilità di un evento dannoso)*		
	RISCHIO TOTALE	**2 TRASCURABILE**		
	Criteri PIA	Trattamento che non comporta due o più dei criteri previsti dal WP29 (GDPR Art.35 e linee guida pia): trattamenti valutativi/scoring; decisioni automatizzate; monitoraggio sistematico; uso dati critici; trattamenti su larga scala; raffronti incrociati di dati; dati di soggetti vulnerabili; uso di tecnologie innovative; trattamenti interdittivi.		
PRINCIPI DI LICEITA' E SICUREZZA	**Principi generali**	Trattamento che soddisfa i principi generali ed i requisiti di liceità (GDPR, Art.5,6): obblighi contrattuali e precontrattuali; obblighi di legge; consenso; legittimo interesse		
	Privacy by design/default	Trattamento che soddisfa i requisiti di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (GDPR, Art.25): quantità di dati raccolti, portata del trattamento, accessibilità, conservazione, ecc.		
	Sicurezza	Trattamento oggetto di adeguate misure tecniche ed organizzative di sicurezza (GDPR, Art.32): vedi "VDS-1-Regolamento videosorveglianza", Cap.6 del presente allegato ed eventuali approfondimenti nelle NOTE		
VALUTAZIONE FINALE		Trattamento che può iniziare / procedere (**rischio mitigato da piano sicurezza**)	Trattamento da sottoporre ad ulteriori valutazioni di impatto	Trattamento da sottoporre a consultazione preventiva dell'Autorità Garante
		X		
NOTE				

ATTIVITA' DI TRATTAMENTO	**Nome**	**Accesso alle registrazioni**		
	Descrizione	Consultazione delle immagini presenti nella memoria delle registrazioni; attività da svolgersi esclusivamente in relazione alle finalità del sistema		
PROFILI DEL TRATTAMENTO	**Categorie di dati**	Immagini videosorveglianza		
	Soggetti interessati	Soggetti ripresi dalle telecamere di videosorveglianza		
	Finalità	Sicurezza e tutela del patrimonio		
	Conservazione	72 ore		
SOGGETTI COINVOLTI	**Autorizzati**	Paolo COSTA; Marco DODICI; Stefano CHIESA; Raffaella FERRARONI; Patrizia TAFURI		
	Destinatari	Trattamento del dato prevalentemente interno (con possibile conoscibilità all'esterno solo per obblighi di legge o contrattuali, di norma senza attività di elaborazione da parte dei soggetti esterni)		
	Responsabili esterni	n/a		
	Contitolare	n/a		
	Diffusione	Non sono oggetto di diffusione		
	Trasferimenti all'estero	n/a		
	Base del trasferimento	n/a		
STRUMENTI	**Repository**	Utilizzo di strumenti digitali (file, cartelle, database, ecc.) di norma su rete o infrastrutture di back-up interne o collocate in cloud in paesi UE o comunque ritenuti adeguati		
CALCOLO DEL LIVELLO DI RISCHIO E VALUTAZIONI DI IMPATTO	**GRAVITÀ**	2 *(valore assegnato in relazione alla natura del dato)*		
	PROBABILITÀ	1 *(valore assegnato in relazione alla probabilità di un evento dannoso)*		
	RISCHIO TOTALE	**2 TRASCURABILE**		
	Criteri PIA	Trattamento che non comporta due o più dei criteri previsti dal WP29 (GDPR Art.35 e linee guida pia): trattamenti valutativi/scoring; decisioni automatizzate; monitoraggio sistematico; uso dati critici; trattamenti su larga scala; raffronti incrociati di dati; dati di soggetti vulnerabili; uso di tecnologie innovative; trattamenti interdittivi.		
PRINCIPI DI LICEITA' E SICUREZZA	**Principi generali**	Trattamento che soddisfa i principi generali ed i requisiti di liceità (GDPR, Art.5,6): obblighi contrattuali e precontrattuali; obblighi di legge; consenso; legittimo interesse		
	Privacy by design/default	Trattamento che soddisfa i requisiti di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (GDPR, Art.25): quantità di dati raccolti, portata del trattamento, accessibilità, conservazione, ecc.		
	Sicurezza	Trattamento oggetto di adeguate misure tecniche ed organizzative di sicurezza (GDPR, Art.32): vedi "VDS-1-Regolamento videosorveglianza", Cap.6 del presente allegato ed eventuali approfondimenti nelle NOTE		
VALUTAZIONE FINALE		Trattamento che può iniziare / procedere (**rischio mitigato da piano sicurezza**)	Trattamento da sottoporre ad ulteriori valutazioni di impatto	Trattamento da sottoporre a consultazione preventiva dell'Autorità Garante
		X		
NOTE				

ATTIVITÀ' DI TRATTAMENTO	**Nome**	**Estrazione di immagini**		
	Descrizione	Estrazione di filmati o singoli frame dalla memoria delle registrazioni; attività da svolgersi esclusivamente in relazione alle finalità del sistema		
PROFILI DEL TRATTAMENTO	**Categorie di dati**	Immagini videosorveglianza		
	Soggetti interessati	Soggetti ripresi dalle telecamere di videosorveglianza		
	Finalità	Sicurezza e tutela del patrimonio		
	Conservazione	72 ore		
SOGGETTI COINVOLTI	**Autorizzati**	Paolo COSTA; Marco DODICI; Stefano CHIESA; Raffaella FERRARONI; Patrizia TAFURI		
	Destinatari	Trattamento del dato prevalentemente interno (con possibile conoscibilità all'esterno solo per obblighi di legge o contrattuali, di norma senza attività di elaborazione da parte dei soggetti esterni)		
	Responsabili esterni	n/a		
	Contitolare	n/a		
	Diffusione	Non sono oggetto di diffusione		
	Trasferimenti all'estero	n/a		
	Base del trasferimento	n/a		
STRUMENTI	**Repository**	Utilizzo di strumenti digitali (file, cartelle, database, ecc.) di norma su rete o infrastrutture di back-up interne o collocate in cloud in paesi UE o comunque ritenuti adeguati		
CALCOLO DEL LIVELLO DI RISCHIO E VALUTAZIONI DI IMPATTO	**GRAVITÀ**	2 *(valore assegnato in relazione alla natura del dato)*		
	PROBABILITÀ	1 *(valore assegnato in relazione alla probabilità di un evento dannoso)*		
	RISCHIO TOTALE	**2 TRASCURABILE**		
	Criteri PIA	Trattamento che non comporta due o più dei criteri previsti dal WP29 (GDPR Art.35 e linee guida pia): trattamenti valutativi/scoring; decisioni automatizzate; monitoraggio sistematico; uso dati critici; trattamenti su larga scala; raffronti incrociati di dati; dati di soggetti vulnerabili; uso di tecnologie innovative; trattamenti interdittivi.		
PRINCIPI DI LICEITA' E SICUREZZA	**Principi generali**	Trattamento che soddisfa i principi generali ed i requisiti di liceità (GDPR, Art.5,6): obblighi contrattuali e precontrattuali; obblighi di legge; consenso; legittimo interesse		
	Privacy by design/default	Trattamento che soddisfa i requisiti di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (GDPR, Art.25): quantità di dati raccolti, portata del trattamento, accessibilità, conservazione, ecc.		
	Sicurezza	Trattamento oggetto di adeguate misure tecniche ed organizzative di sicurezza (GDPR, Art.32): vedi "VDS-1-Regolamento videosorveglianza", Cap.6 del presente allegato ed eventuali approfondimenti nelle NOTE		
VALUTAZIONE FINALE		Trattamento che può iniziare / procedere (**rischio mitigato da piano sicurezza**)	Trattamento da sottoporre ad ulteriori valutazioni di impatto	Trattamento da sottoporre a consultazione preventiva dell'Autorità Garante
		X		
NOTE				

ATTIVITÀ' DI TRATTAMENTO	**Nome**	**Configurazione del sistema**		
	Descrizione	Modifica delle configurazioni del sistema, delle telecamere e del software; attività da svolgersi in coerenza con il regolamento videosorveglianza		
PROFILI DEL TRATTAMENTO	**Categorie di dati**	Dati utenti e log sistema; Immagini videosorveglianza		
	Soggetti interessati	Soggetti ripresi dalle telecamere di videosorveglianza; Utenti		
	Finalità	Operatività del sistema		
	Conservazione	Commisurato alle finalità ed obblighi di legge		
SOGGETTI COINVOLTI	**Autorizzati**	Nessun incaricato interno		
	Destinatari	Trattamento affidato a soggetti / strutture esterne con attività di elaborazione		
	Responsabili esterni	Metronotte Piacenza Srl e Adyda Srl		
	Contitolare	n/a		
	Diffusione	Non sono oggetto di diffusione		
	Trasferimenti all'estero	n/a		
	Base del trasferimento	n/a		
STRUMENTI	**Repository**	Utilizzo di strumenti digitali (file, cartelle, database, ecc.) di norma su rete o infrastrutture di back-up interne o collocate in cloud in paesi UE o comunque ritenuti adeguati		
CALCOLO DEL LIVELLO DI RISCHIO E VALUTAZIONI DI IMPATTO	**GRAVITÀ**	2 *(valore assegnato in relazione alla natura del dato)*		
	PROBABILITÀ	2 *(valore assegnato in relazione alla probabilità di un evento dannoso)*		
	RISCHIO TOTALE	4 LIMITATO		
	Criteri PIA	Trattamento che non comporta due o più dei criteri previsti dal WP29 (GDPR Art.35 e linee guida pia): trattamenti valutativi/scoring; decisioni automatizzate; monitoraggio sistematico; uso dati critici; trattamenti su larga scala; raffronti incrociati di dati; dati di soggetti vulnerabili; uso di tecnologie innovative; trattamenti interdittivi.		
PRINCIPI DI LICEITA' E SICUREZZA	**Principi generali**	Trattamento che soddisfa i principi generali ed i requisiti di liceità (GDPR, Art.5,6): obblighi contrattuali e precontrattuali; obblighi di legge; consenso; legittimo interesse		
	Privacy by design/default	Trattamento che soddisfa i requisiti di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (GDPR, Art.25): quantità di dati raccolti, portata del trattamento, accessibilità, conservazione, ecc.		
	Sicurezza	Trattamento oggetto di adeguate misure tecniche ed organizzative di sicurezza (GDPR, Art.32): vedi "VDS-1-Regolamento videosorveglianza", Cap.6 del presente allegato ed eventuali approfondimenti nelle NOTE		
VALUTAZIONE FINALE		Trattamento che può iniziare / procedere **(rischio mitigato da piano sicurezza)**	Trattamento da sottoporre ad ulteriori valutazioni di impatto	Trattamento da sottoporre a consultazione preventiva dell'Autorità Garante
		X		
NOTE				

ATTIVITA' DI TRATTAMENTO	Nome	Servizi di assistenza tecnica		
	Descrizione	Accesso al sistema per servizi di installazione, configurazione, assistenza, manutenzione impianto		
PROFILI DEL TRATTAMENTO	Categorie di dati	Dati utenti e log sistema; Immagini videosorveglianza		
	Soggetti interessati	Soggetti ripresi dalle telecamere di videosorveglianza; Utenti		
	Finalità	Operatività del sistema		
	Conservazione	Commisurato alle finalità ed obblighi di legge		
SOGGETTI COINVOLTI	Autorizzati	Nessun incaricato interno		
	Destinatari	Trattamento affidato a soggetti / strutture esterne con attività di elaborazione		
	Responsabili esterni	Metronotte Piacenza Srl e Adyda Srl		
	Contitolare	n/a		
	Diffusione	Non sono oggetto di diffusione		
	Trasferimenti all'estero	n/a		
	Base del trasferimento	n/a		
STRUMENTI	Repository	Utilizzo di strumenti digitali (file, cartelle, database, ecc.) di norma su rete o infrastrutture di back-up interne o collocate in cloud in paesi UE o comunque ritenuti adeguati		
CALCOLO DEL LIVELLO DI RISCHIO E VALUTAZIONI DI IMPATTO	GRAVITÀ	2 *(valore assegnato in relazione alla natura del dato)*		
	PROBABILITÀ	2 *(valore assegnato in relazione alla probabilità di un evento dannoso)*		
	RISCHIO TOTALE	3 LIMITATO		
	Criteri PIA	Trattamento che non comporta due o più dei criteri previsti dal WP29 (GDPR Art.35 e linee guida pia): trattamenti valutativi/scoring; decisioni automatizzate; monitoraggio sistematico; uso dati critici; trattamenti su larga scala; raffronti incrociati di dati; dati di soggetti vulnerabili; uso di tecnologie innovative; trattamenti interdittivi.		
PRINCIPI DI LICEITA' E SICUREZZA	Principi generali	Trattamento che soddisfa i principi generali ed i requisiti di liceità (GDPR, Art.5,6): obblighi contrattuali e precontrattuali; obblighi di legge; consenso; legittimo interesse		
	Privacy by design/default	Trattamento che soddisfa i requisiti di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (GDPR, Art.25): quantità di dati raccolti, portata del trattamento, accessibilità, conservazione, ecc.		
	Sicurezza	Trattamento oggetto di adeguate misure tecniche ed organizzative di sicurezza (GDPR, Art.32): vedi "VDS-1-Regolamento videosorveglianza", Cap.6 del presente allegato ed eventuali approfondimenti nelle NOTE		
VALUTAZIONE FINALE		Trattamento che può iniziare / procedere (**rischio mitigato da piano sicurezza**)	Trattamento da sottoporre ad ulteriori valutazioni di impatto	Trattamento da sottoporre a consultazione preventiva dell'Autorità Garante
		X		
NOTE				

Identificazione eventuali altri collegamenti
Il sistema di videosorveglianza, al fine di garantire un più efficace perseguimento delle finalità istituzionali di ordine e sicurezza pubblica, è interfacciato ai seguenti sistemi

SISTEMA	DESCRIZIONE	OWNER
Sistemi polizia locale		
Banche dati nazionali		

4.3) Sicurezza del trattamento

Nel GDPR l'implementazione di adeguate misure di sicurezza a tutela dei dati si colloca alla fine del processo di "responsabilizzazione" (Accountability).

Le misure di sicurezza devono garantire un **livello di sicurezza adeguato al rischio** (art.32, par.1*Art. 32 "Sicurezza del trattamento" 1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto* ***misure tecniche e organizzative*** *adeguate per garantire un livello di sicurezza adeguato al rischio)*

La seguente tabella riporta una sintesi dell misure di sicurezza adottate dal Titolare

TIPOLOGIA	MISURA	DESCRIZIONE
Misure tecniche	Procedure autenticazione	Assegnazione di credenziali univoche agli incaricati
		Criteri di complessità password
		Sostituzione periodica password
		Tracciatura dei log di accesso e delle operazioni compiute (conservazione 1 anno)
	Protezione da malware	Reti informatiche a cui sono connessi agli apparati di ripresa protette dai rischi di accesso abusivo di cui all'art.615-ter, Codice Penale
	Trasmissione sicura dati	Applicazione di tecniche crittografiche alla trasmissione dei dati
	Sicurezza fisica	Apparati di registrazione delle immagini collocati in locali ad accesso sicuro e controllato
		Modalità di collegamento alla visione delle immagini live che garantiscano un'adeguata tutela della riservatezza
Misure organizzative	Responsabilizzazione soggetti	Tutti i soggetti coinvolti hanno ricevuto lettera di autorizzazione e istruzioni Tutti i soggetti coinvolti possono accedere a copia del Regolamento e Manuale operativo comunale di videosorveglianza
	Istruzioni soggetti	
	Procedure gestione	

In relazione all'implementazione delle suddette misure di sicurezza il rischio residuo connesso all'attività di trattamento dati tramite sistemi di videosorveglianza è da considerarsi **accettabile** (valutazione effettuata e verificata periodicamente dal Data Protection Officer).

4.4 Gestione delle violazioni di dati personali (Data Breach, GDPR - Art. 33)

Si ha una "violazione dei dati personali" quando accidentalmente (colposamente) o in modo illecito (dolosamente) un evento causa la distruzione, la perdita, la modifica, la divulgazione non autorizzata, l'accesso ai dati personali trasmessi, conservati o comunque trattati.

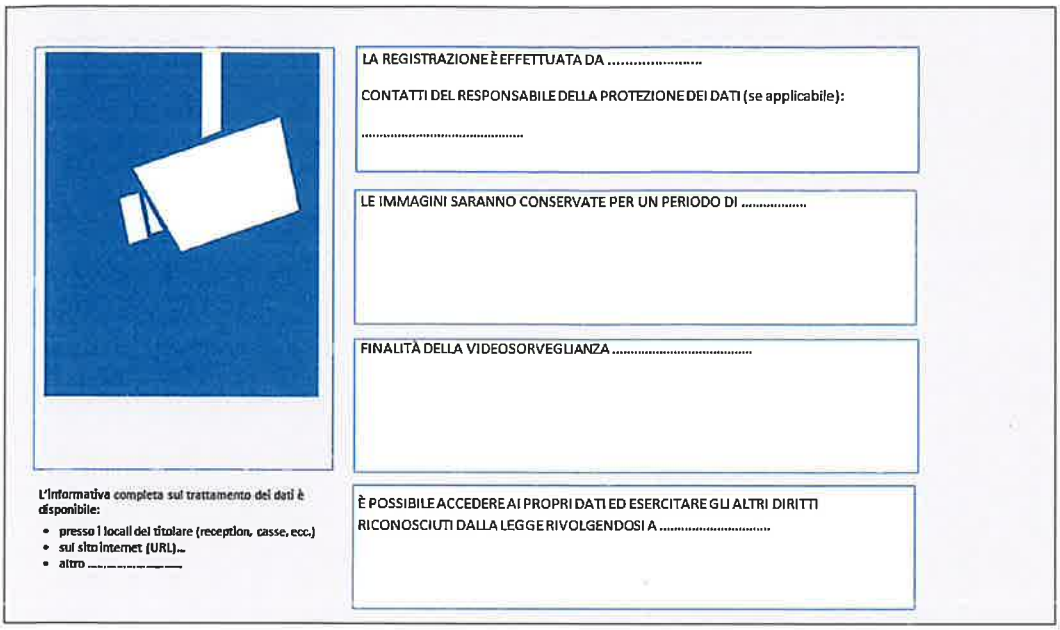
IL GDPR prevede l'obbligo, per tutti i Titolari, di notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (GDPR, considerando 85). Il Titolare provvede in ogni caso a **documentare le violazioni di dati personali subite**, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

In allegato è riportato il "**Registro delle violazioni**", mentre al seguente capitolo la "**Procedura di gestione delle violazioni**".

4.5 Informativa agli interessati

Il Garante ritiene fortemente auspicabile l'utilizzo di appositi cartelli segnaletici finalizzati ad informare gli interessati che transitano nelle aree videosorvegliate. Segnala inoltre modalità semplificate per rendere un'informativa circostanziata maggiormente dettagliata.

FAC-SIMILE CARTELLO "AREA VIDEOSORVEGLIATA"



I cartelli sono collocati nei punti di ingresso del territorio comunale e presso le aree cittadine video sorvegliate.

Il supporto con l'informativa:
- deve essere collocato nei luoghi ripresi o nelle immediate vicinanze, non necessariamente a contatto con la telecamera;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile.

Evidenza del cartello compilato	**VS-C4-Cartello**

INFORMATIVA PUBBLICATA ON LINE
A completamento dell'informativa semplificata fornita tramite cartello viene resa disponibile, tramite pubblicazione sul sito web del Comune, un'informativa circostanziata, completa di tutti gli elementi previsti dall'Art.13 del GDPR.

Testo informativa	**VS-C4-Informativa completa**
Link	

4.6 Diritti degli interessati

Il GDPR, per quanto concerne il tema dei "diritti" degli interessati al trattamento, presenta diversi elementi di continuità con la precedente normativa; il legislatore europeo ha tuttavia introdotto (nell'elencazione che va dall'art. 15 al 22 del GDPR) **nuove prerogative riconosciute agli interessati al trattamento**, tenendo in considerazione l'attuale sviluppo delle nuove tecnologie che potenzialmente possono determinare nuovi pericoli e rischi per i diritti e le libertà degli stessi.

Di seguito viene riportata un'elencazione dei diritti degli interessati previsti dal GDPR (par.3.1), nonché le modalità attuative implementate dal Comune di Gossolengo per fornire un puntuale ed esaustivo riscontro ad eventuali richieste degli interessati (par. 3.2).

DIRITTO	ATTUAZIONE
ART.15 **Diritto di accesso**	Garantito secondo procedura di cui al seguente Capitolo 5
ART.16 **Diritto di rettifica**	Non esercitabile in relazione ad attività di videosorveglianza
ART.17 **Diritto di cancellazione (oblio)**	Non applicabile in relazione ad attività di videosorveglianza (cancellazione entro 7 giorni dall'acquisizione)

ART.18 **Diritto di limitazione**	Non esercitabile in relazione ad attività di videosorveglianza
ART.20 **Diritto alla portabilità dei dati**	Garantito secondo procedura di cui al seguente Capitolo 5
ART.21 **Diritto di opposizione**	Non esercitabile in relazione ad attività di videosorveglianza
ART.22 **Processi decisionali automatizzati (profilazione)**	Non applicabile in relazione ad attività di videosorveglianza

5. ALLEGATI E PROCEDURE OPERATIVE

Il presente capitolo intende fornire sintetici riscontri sulle modalità attuative dei profili di conformità indicati nel presente manuale:

- nomine soggetti coinvolti;
- verifica ed aggiornamento documenti;
- gestione violazioni (data breach);
- gestione richieste diritti degli interessati;
- accesso alle immagini.

5.1 Nomine dei soggetti coinvolti nel sistema

- La scelta e la nomina dei soggetti autorizzati al trattamento è di esclusiva competenza del Titolare del trattamento (Sindaco).
- La nomina deve essere compilata in base al profilo di autorizzazione definito e sottoscritta per accettazione dal soggetto designato.
- La nomina rimane valida per tutto l'arco del rapporto lavorativo (o fino a revoca del Titolare).
- Gli atti di nomina sono conservati insieme al presente fascicolo di conformità.

5.2 Aggiornamento documenti e verifiche misure

Tutta la documentazione rilasciata e relativi contenuti, incluse le misure di sicurezza, sarà oggetto di verifica periodica (audit) almeno annuale, condotto da:
◎ Data Protection Officer
◎ Consulente dedicato
◎ Altro soggetto:

5.3 Gestione violazioni

La seguente tabella identifica la procedura di gestione di eventuali violazioni dei dati (data breach) identificando le fasi, gli strumenti / modalità di gestione ed i soggetti preposti

FASE	STRUMENTI	SOGGETTI
Rilevazione incidenti	Flusso informativo dai soggetti autorizzati e dai responsabili esterni Rilevazioni automatiche da infrastruttura	Autorizzati Resp.esterni DPO
Compilazione registro	Vedi modello allegato **VS-Registro Data Breach**	DPO
Valutazione Impatto	Secondo specifiche di legge	DPO
Notifica al Garante	Vedi modello allegato **VS-Comunicazione Data Breach**	DPO
Notifica agli interessati	Vedi modello allegato **VS-Comunicazione Data Breach**	DPO

5.4 Visione ed utilizzo delle immagini

L'accesso alle **immagini live** può avvenire solamente per la verifica di circostanze collegate al corretto espletamento delle finalità per cui è attivato il sistema. Gli operatori abilitati all'accesso live dovranno garantire la dovuta protezione e riservatezza durante l'accesso.

L'**accesso alle registrazioni**, sia per esigenze di controllo sia in caso di esercizio dei diritti dell'interessato, deve avvenire solo tramite i soggetti depositari delle chiavi di autenticazione idonee. La visione e l'eventuale utilizzo, totale o parziale, delle registrazioni è consentita solo ed esclusivamente (su richieste o disposizioni tracciate e controllate):

- in caso di necessaria verifica di circostanze che potrebbero costituire fattispecie di reato;
- in caso di richiesta di accesso ex.art.15 da parte di soggetti interessati;
- in caso di richiesta da parte dell'Autorità Giudiziaria.

Le immagini non vengono in alcun modo diffuse o comunicate a soggetti terzi non identificati.

Estrazione di immagini dal sistema

In relazione alla verifica di particolari circostanze che potrebbero configurare fattispecie di reato le immagini potranno essere estratte dal sistema e utilizzate/conservate con lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi.

Le immagini possono essere estratte dai supporti di memorizzazione dell'impianto e riversate su un supporto asportabile, solo nei seguenti casi:

1) su richiesta dell'interessato, ai sensi dell'art.20 (*Diritto alla portabilità dei dati*) del GDPR, da effettuarsi previa presentazione di un documento di identità ed adeguata motivazione;
2) su segnalazione da parte degli incaricati di circostanze collegate alle finalità elencate nel presente documento;
3) su richiesta del titolare, in relazione alla verifica di circostanze sospette che possano configurare ipotesi di reato (segnalazioni, rilevazione di indizi di reato, attivazione impianti di allarme, ecc.);
4) su richiesta delle forze dell'ordine o della magistratura.

In tali casi sarà necessario redigere un "**verbale di estrazione**" (allegato **VDS-5-Format accesso estrazione**) che documenti le motivazioni e le modalità delle operazioni effettuate, nonché i criteri adottati al fine di garantire un adeguato livello di protezione e riservatezza delle immagini.

APPENDICE: METODOLOGIA DI VALUTAZIONE DEL RISCHIO

Il GDPR richiede che venga effettuata un'analisi di rischio per tutte le attività di trattamento effettuate dal titolare. Il rischio inerente al trattamento è da intendersi come **rischio di impatti negativi sulle libertà e i diritti degli interessati** (GDPR - Considerando 75-77), derivante da un evento dannoso quale distruzione accidentale o illegale, perdita, modifica, rivelazione o accesso non autorizzato.

Per definire il livello complessivo di rischio, di tali eventi, occorre determinare la **GRAVITA'** e la **PROBABILITA'** di accadimento di un evento dannoso.

GRAVITA' L'indice di gravità di un evento dannoso è calcolato in relazione alla **categoria di dato**, secondo il seguente schema

TIPO DI DATI	CONSEGUENZE	INDICE GRAVITA'
DATI COMUNI SEMPLICI Dati anagrafici, Dati di contatto, Indirizzi posta email, ecc.	**Conseguenze irrilevanti** o limitate, che possono essere superate senza problemi	1 BASSO
DATI COMUNI RILEVANTI Dati economico/finanziari, Rendimento professionale, Estremi documenti identità; **Foto, audio, video**, Dati di traffico e log; Dati relativi all'ubicazione; ecc	**Conseguenze significative**, che possono essere superate con media difficoltà (danni reputazionali, danni economico/sociali, furto identità, ...)	2 MEDIO/BASSO
DATI PARTICOLARI Origine razziale/etnica; Opinioni politiche e appartenenze sindacali; Convinzioni religiose o filosofiche; Dati di salute; Orientamento sessuale; Condanne penali, reati	**Conseguenze gravi**, che possono essere superate con alta difficoltà (discriminazione)	3 MEDIO/ALTO
DATI BIOMETRICI Dati biometrici, Dati genetici	**Conseguenze irreversibili** (gravi disturbi fisici/psicologici, invalidità, morte)	4 ALTO

PROBABILITA' La probabilità di accadimento è calcolata in relazione al numero di soggetti coinvolti nel trattamento ed agli strumenti utilizzati

COMBINAZIONE SOGGETTI/STRUMENTI	INDICE DI PROBABILITA'
Accesso solo soggetti interni (oppure accesso esclusivo a istituto di vigilanza nominato) Strumenti/archiviazione interni Accesso solo presso apparato di registrazione	1 BASSO
Accesso solo soggetti interni Strumenti/archiviazione interni Accesso tramite LAN e/o mobile-device	2 MEDIO / BASSO
Accesso soggetti interni e/o esterni Strumenti/archiviazione interni Accesso tramite LAN e/o mobile-device e/o centrali operative esterne	3 MEDIO / ALTO
Collocazione archiviazione registrazioni esterna	4 ALTO

LIVELLO DI RISCHIO DELLE ATTIVITA' DI TRATTAMENTO

La seguente tabella identifica la modalità di determinazione del livello di rischio complessivo per ogni singola attività di trattamento (come identificato in par.4.2), tramite la combinazione di gravità e probabilità.

GRAVITA' \ PROBABILITA'	1	2	3	4
1	1	2	3	4
2	2	3	4	5
3	3	4	5	6
4	4	5	6	7

LEGENDA SULL'INDICE DI LIVELLO COMPLESSIVO DI RISCHIO:
[1,2] Livello complessivo BASSO
[3,4] Livello complessivo MEDIO/BASSO
[5] Livello complessivo MEDIO/ALTO
[6,7] Livello complessivo ALTO