



COMUNE DI BELFORTE ALL'ISAURO

REGOLAMENTO SULL'UTILIZZO DEI SISTEMI DI VIDEOSORVEGLIANZA DEL COMUNE DI BELFORTE ALL'ISAURO

APPROVATO CON DELIBERA DEL CONSIGLIO COMUNALE N°24 DEL 27/07/2026

Art. 1

Oggetto e ambito di applicazione

1. Il presente regolamento disciplina l'installazione, la gestione e l'utilizzo degli impianti di videosorveglianza di contesto e dei dispositivi di lettura automatica delle targhe installati dal Comune, nel rispetto del Regolamento (UE) 2016/679, del d.lgs. 196/2003, del d.lgs. 51/2018 per i trattamenti svolti per finalità di polizia, del d.l. 11/2009, del d.l. 14/2017, del Codice della strada e dei provvedimenti del Garante per la protezione dei dati personali.
2. Costituisce videosorveglianza il complesso di strumenti finalizzati alla vigilanza a distanza mediante dispositivi di ripresa video, eventualmente integrati da funzioni tecniche di analisi strettamente necessarie, collegati a un centro di controllo e coordinamento gestito dal Comando di Polizia Locale o da altre strutture comunali competenti nei limiti delle attribuzioni organizzative definite dal Comune.
3. Le immagini, qualora rendano le persone identificate o identificabili, costituiscono dati personali. In tali casi la videosorveglianza incide sul diritto delle persone alla propria riservatezza.
4. Il sistema comunale è composto da n. 3 telecamere di contesto, n.2 dispositivi OCR/ANPR, sistemi di registrazione, client autorizzati, log e misure di sicurezza tecniche e organizzative.

Art. 2

Principi generali

Si riassumono di seguito i principi per la gestione dei sistemi/impianti e per il trattamento dei dati:

1. **Principio di liceità:** il trattamento di dati personali effettuato attraverso sistemi di videosorveglianza da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali. Esso infatti è necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui il Comune e il comando di polizia locale sono investiti.
2. **Principio di necessità:** i sistemi di videosorveglianza sono configurati per l'utilizzazione al minimo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
3. **Principio di proporzionalità:** nel commisurare la necessità del sistema di videosorveglianza al grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra una effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti.
4. **Principio di finalità:** gli scopi perseguiti devono essere determinati, espliciti e legittimi.

Art. 3

Soggetti

1. Titolare del trattamento dei dati personali.
Il Titolare del trattamento dei dati personali rilevati con i sistemi di videosorveglianza, disciplinati dal presente Regolamento, è il Comune di Bleforte all'Isauro, rappresentato dal Sindaco pro tempore, che definisce autonomamente le modalità, le garanzie e i limiti di trattamento dei dati personali, ed elabora specifici modelli organizzativi che ne garantiscono una costante applicazione e monitoraggio.

2. Il Responsabile della protezione dei dati (RPD/DPO) svolge i compiti previsti dagli artt. 37-39 GDPR. Non svolge funzioni operative sul sistema e non accede ordinariamente alle immagini; nell'ambito di audit e verifiche acquisisce soltanto le evidenze strettamente necessarie.

3. Soggetti autorizzati e profili di accesso.

L'accesso ai sistemi e ai dati è consentito solo a soggetti formalmente autorizzati e istruiti, con credenziali personali, profili differenziati e principio del minimo privilegio.

Gli autorizzati operano sulla base di istruzioni scritte periodicamente aggiornate e sono soggetti a specifica formazione.

Le operazioni consentite sono limitate a visione live, visione differita, ricerca transiti, estrazione e trasmissione all'autorità competente, secondo il profilo assegnato.

È vietata la condivisione delle credenziali e ogni consultazione per curiosità o fini personali.

4. I fornitori che trattano dati personali per conto del Comune sono nominati responsabili del trattamento con atto conforme all'art. 28 GDPR.

5. Manutenzione, amministratori di sistema e responsabili esterni.

Gli amministratori di sistema e i tecnici manutentori sono individuati nominativamente e operano nei limiti delle attività affidate.

Gli accessi tecnici da remoto sono ammessi soltanto mediante VPN o canali equivalenti sicuri, con tracciatura completa e, ove possibile, presidio di personale comunale autorizzato.

I fornitori che trattano dati per conto del Comune sono nominati responsabili del trattamento con specifiche istruzioni.

Art. 4

Finalità dei sistemi e architettura degli impianti

1. Il trattamento è effettuato esclusivamente per finalità determinate, esplicite e legittime, strettamente connesse ai compiti istituzionali del Comune e della Polizia Locale, nel rispetto del principio di limitazione della finalità.

In particolare, le telecamere di contesto sono utilizzate per:

- presidio di aree pubbliche o aperte al pubblico individuate dal Comune per finalità di sicurezza urbana, nel quadro del Patto stipulato con la Prefettura;
- tutela del patrimonio comunale e prevenzione di danneggiamenti, atti vandalici, condotte illecite e situazioni di degrado;
- supporto alla ricostruzione di eventi dannosi o illeciti già verificatisi;
- tutela della viabilità e della sicurezza stradale nei limiti delle competenze attribuite;
- tutela ambientale e contrasto di specifici fenomeni illeciti, in presenza di una norma attributiva del compito e di una valutazione della proporzionalità.

I dispositivi di lettura targhe sono utilizzati esclusivamente per:

- rilevare il transito dei veicoli ai varchi individuati dall'Ente;
- supportare, nei limiti consentiti dalla legge, le attività di controllo connesse alla circolazione stradale e agli ulteriori compiti attribuiti alla Polizia Locale;
- verificare, nei casi e nei limiti normativamente consentiti, la sussistenza di alert o segnalazioni legittimamente trattabili nell'ambito delle funzioni istituzionali;
- supportare le attività di sicurezza urbana, prevenzione e accertamento nei limiti delle competenze esercitate.

Non sono consentiti usi ulteriori incompatibili con le finalità sopra indicate. In particolare, il sistema non è utilizzato per riconoscimento facciale, identificazione biometrica, sorveglianza generalizzata dei comportamenti, profilazione individuale o ricostruzione sistematica dei percorsi delle persone fisiche al di fuori dei casi strettamente consentiti dall'ordinamento

2. Per i trattamenti rientranti nel perimetro del GDPR, la base giuridica del trattamento è l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Comune e, per quanto di competenza, la Polizia Locale, ai sensi dell'art. 6, par. 1, lett. e) del Regolamento (UE) 2016/679, in combinazione con la normativa nazionale e regolamentare che attribuisce all'Ente i compiti istituzionali in materia di sicurezza urbana, viabilità, tutela del patrimonio, presidio del territorio e accertamento di illeciti amministrativi.

3. Per i trattamenti ricadenti nell'ambito di applicazione del d.lgs. 51/2018, il presupposto di liceità è costituito dall'esercizio delle funzioni di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nei limiti delle attribuzioni concretamente spettanti alla Polizia Locale quale autorità competente.

4. Il consenso dell'interessato non costituisce base giuridica del trattamento e non è richiesto, trattandosi di trattamento fondato su compiti di interesse pubblico e pubblici poteri.

5. Le finalità di cui al presente articolo costituiscono la cornice generale di liceità del sistema. La concreta attivazione di ciascun punto di ripresa o varco è subordinata a specifica istruttoria tecnica e giuridica che ne motivi necessità, proporzionalità, ubicazione, angolo di ripresa e coerenza con le finalità effettivamente perseguite.

Art. 5

Divieti e limiti

1. È vietato ogni utilizzo incompatibile con le finalità di cui al presente regolamento.
2. È vietato l'uso del sistema per riconoscimento facciale, trattamento di dati biometrici, profilazione sistematica delle persone o ricostruzione generalizzata dei percorsi individuali.
3. La mera disponibilità tecnica di funzioni ulteriori del software o del dispositivo non legittima il loro utilizzo da parte del Comune.
4. Gli impianti di videosorveglianza non possono essere utilizzati, in base alla vigente normativa, sulla tutela dei diritti dei lavoratori per effettuare controlli sull'attività lavorativa dei dipendenti del Comune, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

Art. 6

Patto con la Prefettura e coordinamento istituzionale

1. Quando il sistema o una sua parte è utilizzato per finalità di sicurezza urbana ai sensi del d.l. 14/2017, il Comune opera nel quadro del patto per l'attuazione della sicurezza urbana sottoscritto con la Prefettura territorialmente competente.
2. Ogni ampliamento significativo delle aree presidiate, del numero dei varchi OCR/ANPR, delle finalità o dei flussi informativi verso le forze di polizia è preceduto dalla verifica di coerenza con il patto vigente e, ove necessario, dal suo aggiornamento.
3. Il presente regolamento non abilita, da solo, l'accertamento automatico delle violazioni del Codice della strada quando la legge richieda ulteriori presupposti di omologazione, approvazione o particolari modalità di contestazione.

Art. 7

Trattamento e conservazione dei dati

1. Le immagini di contesto e i dati ordinari di transito sono conservati per un termine ordinario non superiore a sette giorni successivi alla rilevazione.

Una conservazione ulteriore è ammessa esclusivamente in presenza di specifiche e documentate esigenze istruttorie o investigative, su richiesta dell'Autorità giudiziaria, della polizia giudiziaria o in relazione a fatti specificamente individuati già emersi entro il termine ordinario di conservazione. L'estensione della conservazione non può essere disposta in via generalizzata o preventiva, ma deve essere puntualmente motivata, tracciata e limitata al tempo strettamente necessario rispetto alla finalità che la giustifica.

3. La cancellazione avviene automaticamente sui sistemi server/NVR allo scadere del termine di conservazione.

4. Le copie estratte su postazioni client o supporti esterni sono consentite solo se motivate, registrate, cifrate quando tecnicamente possibile e cancellate o distrutte senza ritardo al venir meno della finalità che ne ha giustificato la creazione.

5. I log di accesso e delle operazioni sono conservati, di regola, per 180 giorni, salvo diverso termine motivato.

Art. 8

Principi di configurazione privacy by design e by default

1. Il sistema è configurato secondo i principi di necessità, proporzionalità, minimizzazione e limitazione della conservazione:

- inquadratura limitata alle aree pertinenti e utilizzo di mascherature privacy ove necessario;
- assenza di audio;
- segmentazione di rete, autenticazione individuale, logging e protocolli sicuri;
- disabilitazione delle funzioni non strettamente necessarie.

Art. 9

Comunicazione, accesso e messa a disposizione dei dati alle autorità

1. Le immagini, i dati di transito, i log e gli estratti possono essere comunicati o messi a disposizione esclusivamente ai soggetti pubblici legittimati dalla legge, all'autorità giudiziaria, alla polizia giudiziaria, alle forze di polizia e alle altre autorità competenti, nei casi e nei limiti previsti dall'ordinamento.

2. La trasmissione o l'accesso avvengono, di regola, su richiesta scritta, motivata e protocollata, con indicazione dell'ufficio richiedente, della base giuridica, dell'oggetto, del periodo temporale e della finalità istituzionale perseguita. Nei casi di urgenza operativa la richiesta può essere anticipata con modalità idonee e successivamente formalizzata senza ritardo. La richiesta motivata può essere sostituita da diverso titolo idoneo previsto dalla legge.

Art. 10

Informativa e trasparenza

1. Il Comune assicura agli interessati un'informativa di primo livello mediante cartelli collocati prima del raggio di azione delle telecamere o dei varchi, anche nelle sue immediate vicinanze, e non necessariamente a contatto con gli impianti, nonché un'informativa estesa consultabile e reperibile sul sito istituzionale e presso il Comando di polizia locale.
2. L'informativa estesa deve indicare almeno il titolare del trattamento, i contatti del RPD, le finalità, la base giuridica, i tempi di conservazione, i destinatari dei dati, le modalità di esercizio dei diritti, il diritto di proporre reclamo al Garante e l'eventuale diverso regime applicabile ai trattamenti ricadenti nel d.lgs. 51/2018.

Art. 11

Distinzione tra i diversi regimi di accesso

1. Le richieste degli interessati aventi ad oggetto dati personali trattati mediante videosorveglianza sono esaminate secondo il Regolamento (UE) 2016/679.
2. Le istanze di esercizio dei diritti privacy sono tenute distinte dall'accesso documentale di cui alla legge n. 241/1990 e dall'accesso civico generalizzato di cui al d.lgs. 33/2013. Il presente regolamento esclude che le immagini siano rilasciate a privati mediante accesso civico generalizzato quando ciò comporti diffusione illecita di dati personali o pregiudizio ai diritti e alle libertà altrui.

Art. 12

Esercizio dei diritti degli interessati nei trattamenti soggetti al GDPR

1. L'interessato può esercitare nei confronti del Comune i diritti previsti dagli articoli 15, 16, 17, 18 e 21 del Regolamento (UE) 2016/679, nei limiti in cui essi siano compatibili con la natura del trattamento, con i termini di conservazione e con l'eventuale sussistenza delle limitazioni previste dall'articolo 23 del Regolamento e dall'articolo 2-undecies del d.lgs. 196/2003.
2. L'istanza non richiede una motivazione sostanziale né la dimostrazione di uno specifico interesse giuridico, ma deve contenere elementi sufficienti a consentire l'individuazione del dato richiesto, quali, ove disponibili, data, fascia oraria, luogo, descrizione della persona o del veicolo e recapito per il riscontro.
3. Il Comune può richiedere esclusivamente le informazioni supplementari necessarie a confermare l'identità del richiedente, quando sussistano ragionevoli dubbi sulla sua identità, nonché a circoscrivere la ricerca delle immagini e dei dati.
4. Il riscontro è fornito senza ingiustificato ritardo e, di norma, entro un mese dal ricevimento dell'istanza; tale termine può essere prorogato nei casi di particolare complessità nei limiti consentiti dalla normativa vigente, con comunicazione motivata all'interessato.
5. L'accesso dell'interessato ai propri dati personali non coincide con il diritto a ottenere indiscriminatamente copia integrale delle registrazioni. Il Comune individua la modalità meno invasiva idonea a soddisfare la richiesta, privilegiando, secondo i casi, la visione assistita, il rilascio di fotogrammi o estratti pertinenti, ovvero di copie con oscuramento o mascheramento dei terzi.
6. Quando l'accoglimento della richiesta possa incidere sui diritti e sulle libertà di altre persone, il Comune procede a un bilanciamento caso per caso e adotta, ove tecnicamente e organizzativamente sostenibili, misure di minimizzazione e oscuramento.

7. L'eventuale diniego totale o parziale, il differimento o la limitazione dell'esercizio dei diritti sono adottati con atto motivato, recante l'indicazione dei mezzi di tutela esperibili, salvo che la motivazione stessa debba essere omessa o limitata per legge.

Art. 13

Accesso alle immagini e ai dati da parte dei cittadini

1. Il cittadino che ritenga di essere stato ripreso o coinvolto in un evento rilevato dal sistema può presentare istanza di accesso ai propri dati personali ai sensi della disciplina privacy applicabile, utilizzando il modulo predisposto dal Comune o altra istanza equivalente.
2. L'istanza deve pervenire con tempestività compatibile con i tempi di conservazione, fermo restando che la scadenza del termine di conservazione e la cancellazione automatica delle registrazioni possono rendere oggettivamente impossibile il riscontro.
3. Le richieste di privati dirette a ottenere immagini o dati riferiti prevalentemente a terzi, ovvero richieste generiche, indeterminate o non riferite ai dati personali del richiedente, non sono accolte tramite il diritto di accesso ai dati personali. Resta ferma la possibilità di acquisizione nell'ambito di procedimenti giudiziari o investigativi nei modi previsti dalla legge.
4. Qualora il Comune riceva istanze impropriamente qualificate come accesso documentale o accesso civico ma aventi in realtà a oggetto l'esercizio dei diritti dell'interessato sui propri dati personali, provvede a trattarle secondo la disciplina privacy, dandone comunicazione al richiedente.

Art.14

Esercizio dei diritti nei trattamenti soggetti al d.lgs. 51/2018

1. Per i trattamenti effettuati dalla polizia locale in qualità di autorità competente per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, si applicano gli articoli 9, 10, 11, 12, 13 e 14 del d.lgs. 51/2018.
2. In tali casi l'interessato ha diritto di ottenere conferma dell'esistenza di un trattamento che lo riguarda, l'accesso ai dati personali, la rettifica dei dati inesatti, nonché, nei casi previsti dalla legge, la cancellazione o la limitazione del trattamento, fatti salvi i limiti e i differimenti necessari a non compromettere indagini, accertamenti, attività processuali o altri interessi pubblici protetti.
3. Il Comune, tramite il Comando di polizia locale, facilita l'esercizio dei diritti, fornisce le informazioni dovute in forma concisa, intellegibile e facilmente accessibile e informa per iscritto l'interessato dell'esito della richiesta senza ingiustificato ritardo.
4. Nei casi previsti dall'articolo 14 del d.lgs. 51/2018, il differimento, la limitazione o il diniego sono adottati con provvedimento motivato nei limiti consentiti dalla legge. L'interessato è informato della facoltà di esercitare i diritti anche tramite il Garante per la protezione dei dati personali ai sensi dell'articolo 13 del medesimo decreto, salvo i casi di trattamento effettuato dall'autorità giudiziaria.

Art. 15

Accesso, consultazione e acquisizione da parte dell'autorità giudiziaria, della polizia giudiziaria e delle forze di polizia

1. L'autorità giudiziaria, la polizia giudiziaria e le forze di polizia possono accedere alle immagini e ai dati o acquisirne copia nei casi previsti dalla legge e per finalità istituzionali di prevenzione,

accertamento e repressione degli illeciti, nel rispetto dei principi di pertinenza, non eccedenza e tracciabilità.

2. L'accesso diretto ai sistemi da parte di soggetti esterni costituisce modalità eccezionale ed è ammesso solo se previsto da specifica base giuridica o da atto convenzionale o organizzativo che disciplini puntualmente ruoli, presupposti, profili autorizzativi, misure di sicurezza, logging, tempi di conservazione e responsabilità. In mancanza, il rilascio avviene mediante estrazione o messa a disposizione controllata da parte del personale comunale autorizzato.

3. Ogni richiesta o consultazione è registrata in apposito log o registro, con indicazione del soggetto richiedente, del presupposto giuridico, dell'oggetto, del periodo interessato, del nominativo dell'operatore che ha eseguito l'estrazione o consentito la consultazione e dell'esito.

4. Nei casi di urgenza, l'accesso o la messa a disposizione possono essere assicurati con priorità, fermo l'obbligo di successiva regolarizzazione documentale e di annotazione delle attività svolte.

Art. 16

Regole procedurali comuni e cautele operative

1. Le istanze degli interessati e le richieste provenienti da autorità o uffici pubblici sono gestite secondo procedure interne che assicurano protocollazione, verifica dell'identità e della legittimazione del richiedente, tempestiva ricerca dei dati, valutazione del bilanciamento con i diritti dei terzi, registrazione dell'esito e conservazione della relativa documentazione.

2. La visione o il rilascio di immagini o dati personali avvengono, ove possibile, presso ambienti controllati, su postazioni dedicate e con modalità tali da evitare accessi indebiti, duplicazioni non autorizzate o diffusioni improprie.

3. Le copie o gli estratti rilasciati sono limitati a quanto strettamente pertinente e recano, ove necessario, oscuramenti, watermark, password, cifratura o altre misure idonee a prevenire ulteriori trattamenti non autorizzati.

4. Il Comune adotta modelli standard per l'esercizio dei diritti degli interessati, per le richieste delle autorità e per i verbali di visione o consegna, assicurando il coinvolgimento del DPO/RPD nei casi di particolare complessità o di dubbia qualificazione giuridica della richiesta.

Art. 17

Riesame e allegati tecnici

1. Il presente regolamento è riesaminato almeno ogni due anni o in caso di modifiche normative, tecnologiche o organizzative rilevanti.

2. Costituiscono allegati tecnici: planimetria dei punti di ripresa, elenco aree monitorate, matrice ruoli/permessi, procedura diritti, informative.

Art. 18

Entrata in vigore

Il presente Regolamento entra in vigore il giorno successivo dalla sua pubblicazione.

Art.19

Norme di rinvio

Per tutto quanto non disciplinato dal presente Regolamento si fa rinvio alle leggi vigenti, ai provvedimenti attuativi delle medesime, alle decisioni del Garante per la protezione dei dati personali e ad ogni altra normativa speciale, generale, nazionale e comunitaria in materia di protezione e trattamento dei dati personali nell'ambito della videosorveglianza.