COMUNE DI VILLAR PELLICE - Prot 0006396 del 22/10/2026 Tit 1 Cl 1 Fasc

COMUNE DI VILLAR PELLICE

Città Metropolitana di Torino

REGOLAMENTO COMUNALE SULLA VIDEOSORVEGLIANZA

Adeguato al Regolamento (UE) 2016/679 (GDPR), al D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018,
al D.L. 14/2017 conv. in L. 48/2017, al Regolamento (UE) 2024/1689 (AI Act) e alla L. 132/2025,
alle Linee guida EDPB 3/2019 e al Provvedimento del Garante del 26 novembre 2020 (FAQ videosorveglianza)

Approvato con deliberazione del Consiglio Comunale n. ___ del __.__.2026

COMUNE DI VILLAR PELLICE - Prot 0006396 del 22/10/2026 Tit 1 Cl 1 Fasc

Indice

Capo I – Principi generali

Art. 1 – Oggetto e finalità del Regolamento

Art. 2 – Ambito di applicazione

Art. 3 – Quadro normativo di riferimento

Art. 4 – Definizioni

Art. 5 – Principi applicabili al trattamento e base giuridica

Art. 6 – Finalità del trattamento

Capo II – Soggetti, adempimenti e responsabilità

Art. 7 – Titolare del trattamento

Art. 8 – Responsabile della protezione dei dati (RPD/DPO)

Art. 9 – Soggetti autorizzati al trattamento e amministratori di sistema

Art. 10 – Responsabili del trattamento ex art. 28 GDPR

Art. 11 – Registro delle attività di trattamento

Art. 12 – Valutazione d'impatto sulla protezione dei dati (DPIA)

Capo III – Modalità del trattamento

Art. 13 – Informativa agli interessati

Art. 14 – Modalità di raccolta delle immagini e requisiti degli impianti

Art. 15 – Conservazione e cancellazione dei dati

Art. 16 – Misure di sicurezza

Art. 17 – Violazioni di dati personali (data breach)

Art. 18 – Obblighi degli operatori

Capo IV – Diritti dell'interessato e comunicazione dei dati

Art. 19 – Diritti dell'interessato

Art. 20 – Comunicazione dei dati e accesso da parte dell'autorità giudiziaria e delle forze di polizia

Capo V – Trattamenti particolari

Art. 21 – Videosorveglianza per finalità di sicurezza urbana e controllo integrato del territorio

Art. 22 – Sistemi di lettura automatica delle targhe (ANPR/LPR)

Art. 23 – Divieto di identificazione biometrica e sistemi di intelligenza artificiale

Art. 24 – Impianti temporanei e mobili

COMUNE DI VILLAR PELLICE - Prot 0006396 del 22/10/2026 Tit 1 Cl 1 Fasc

Capo VI – Norme finali

Art. 25 – Provvedimenti attuativi

Art. 26 – Sanzioni

Art. 27 – Norme di rinvio e adeguamento automatico

Art. 28 – Pubblicità del Regolamento

Art. 29 – Abrogazioni ed entrata in vigore

Allegato A – Modello di informativa minima (cartello di area videosorvegliata)

COMUNE DI VILLAR PELLICE - Prot 0006396 del 22/10/2026 Tit 1 Cl 1 Fasc

CAPO I – PRINCIPI GENERALI

Art. 1 – Oggetto e finalità del Regolamento

1. Il presente Regolamento disciplina il trattamento dei dati personali effettuato dal Comune di Villar Pellice mediante sistemi di videosorveglianza installati e gestiti sul territorio comunale, garantendo che esso si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea.

2. Il Regolamento costituisce, altresì, misura di garanzia e di accountability ai sensi degli artt. 5, par. 2, e 24 del Regolamento (UE) 2016/679 (di seguito "GDPR"), documentando le scelte organizzative e tecniche adottate dal Titolare del trattamento.

Art. 2 – Ambito di applicazione

1. Il presente Regolamento si applica a tutti i trattamenti di dati personali effettuati mediante sistemi di videosorveglianza, fissi o mobili, attivati nel territorio comunale dal Comune di Villar Pellice in qualità di Titolare del trattamento, ivi compresi i sistemi collegati alla centrale di controllo, i sistemi di ripresa presso immobili di proprietà o in uso all'Ente e gli eventuali dispositivi temporanei.

2. Sono esclusi dall'ambito di applicazione del presente Regolamento i trattamenti effettuati da soggetti privati o da altri titolari pubblici, nonché i trattamenti effettuati dalle Forze di Polizia dello Stato per finalità di prevenzione, indagine, accertamento e perseguimento di reati, disciplinati dal D.Lgs. 18 maggio 2018, n. 51, di attuazione della Direttiva (UE) 2016/680.

3. I trattamenti effettuati dalla Polizia Locale per le finalità di cui al D.Lgs. 51/2018 sono svolti nel rispetto della predetta normativa; per quanto compatibili, si applicano le misure organizzative e di sicurezza previste dal presente Regolamento.

Art. 3 – Quadro normativo di riferimento

1. Il presente Regolamento è adottato in conformità e in attuazione delle seguenti fonti, come tempo per tempo vigenti:

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR);
- D.Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), come modificato dal D.Lgs. 10 agosto 2018, n. 101;
- D.Lgs. 18 maggio 2018, n. 51, di attuazione della Direttiva (UE) 2016/680 (trattamenti per finalità di polizia e giustizia penale);
- D.L. 20 febbraio 2017, n. 14, convertito con modificazioni dalla L. 18 aprile 2017, n. 48 (disposizioni urgenti in materia di sicurezza delle città), e successive modificazioni, ivi incluso il D.L. 4 ottobre 2018, n. 113, convertito dalla L. 1 dicembre 2018, n. 132;
- Regolamento (UE) 2024/1689 del 13 giugno 2024 (Regolamento sull'intelligenza artificiale – "AI Act"), con particolare riferimento alle pratiche vietate di cui all'art. 5;
- L. 23 settembre 2025, n. 132 (disposizioni nazionali in materia di intelligenza artificiale);
- Linee guida 3/2019 del Comitato europeo per la protezione dei dati (EDPB) sul trattamento dei dati personali attraverso dispositivi video, versione 2.0 del 29 gennaio 2020;
- Provvedimento del Garante per la protezione dei dati personali del 26 novembre 2020 (FAQ in materia di videosorveglianza) e ulteriori provvedimenti generali dell'Autorità in materia;
- Provvedimento del Garante del 27 novembre 2008 in materia di amministratori di sistema, e successive modificazioni;
- D.Lgs. 18 agosto 2000, n. 267 (Testo unico delle leggi sull'ordinamento degli enti locali); L. 7 marzo 1986, n. 65 (ordinamento della Polizia Municipale); L.R. Piemonte 9 agosto 1988, n. 40; L. 20 maggio 1970, n. 300 (Statuto dei lavoratori), con particolare riferimento all'art. 4 in materia di controlli a distanza dei lavoratori.

2. Il Provvedimento generale del Garante in materia di videosorveglianza dell'8 aprile 2010 si intende richiamato nei soli limiti in cui risulti compatibile con il GDPR, secondo quanto chiarito dal Garante medesimo e dalle Linee guida EDPB 3/2019.

Art. 4 – Definizioni

1. Ai fini del presente Regolamento, si intende per:

a) "dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"), anche indirettamente, rilevata mediante le riprese effettuate dall'impianto di videosorveglianza, ai sensi dell'art. 4, n. 1, GDPR;

b) "trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, quali la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, n. 2, GDPR);

c) "titolare del trattamento": il Comune di Villar Pellice, che determina le finalità e i mezzi del trattamento (art. 4, n. 7, GDPR);

d) "responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare (art. 4, n. 8, GDPR), designato con atto giuridico conforme all'art. 28 GDPR;

e) "soggetto autorizzato": la persona fisica che, operando sotto l'autorità diretta del Titolare o del Responsabile, è autorizzata e istruita a trattare i dati personali ai sensi degli artt. 4, n. 10, e 29 GDPR e dell'art. 2-quaterdecies del Codice;

f) "responsabile della protezione dei dati" (RPD o DPO): il soggetto designato dal Titolare ai sensi degli artt. 37-39 GDPR;

g) "interessato": la persona fisica cui si riferiscono i dati personali oggetto di trattamento;

h) "comunicazione": il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dai soggetti autorizzati e dal responsabile, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

i) "diffusione": il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma;

j) "violazione dei dati personali" (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 (art. 4, n. 12, GDPR);

k) "dato biometrico": il dato personale ottenuto da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consente o conferma l'identificazione univoca (art. 4, n. 14, GDPR);

l) "sistema di identificazione biometrica remota": il sistema di IA finalizzato all'identificazione di persone fisiche, senza il loro coinvolgimento attivo, tipicamente a distanza, mediante confronto dei dati biometrici con quelli contenuti in una banca dati di riferimento (art. 3 Reg. UE 2024/1689);

m) "videosorveglianza": il trattamento di dati personali effettuato mediante sistemi di ripresa video, con o senza registrazione delle immagini;

n) "GDPR": il Regolamento (UE) 2016/679; "Codice": il D.Lgs. 196/2003 e s.m.i.; "Garante": il Garante per la protezione dei dati personali.

Art. 5 – Principi applicabili al trattamento e base giuridica

1. Il trattamento dei dati personali mediante sistemi di videosorveglianza è improntato ai principi di cui all'art. 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza; responsabilizzazione (accountability).

2. La base giuridica del trattamento è costituita dall'art. 6, par. 1, lett. e), GDPR (esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare), in combinato disposto con l'art. 2-ter del Codice, sussistendo il fondamento nelle norme di legge e di regolamento che attribuiscono al Comune le funzioni istituzionali di cui al successivo art. 6, nonché nel presente Regolamento. Il trattamento non richiede il consenso dell'interessato.

3. In applicazione dei principi di minimizzazione e di protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 GDPR), i sistemi sono configurati in modo da limitare la raccolta ai soli dati pertinenti e non eccedenti rispetto alle finalità

perseguite, escludendo le riprese non necessarie: l'angolo visuale delle telecamere è limitato alle aree di effettivo interesse, con oscuramento automatico (privacy masking) delle aree private e delle porzioni di territorio non pertinenti.

4. L'installazione di sistemi di videosorveglianza è disposta solo qualora altre misure, ponderatamente valutate, risultino insufficienti o inattuabili (principio di proporzionalità). La valutazione di proporzionalità è documentata nell'istruttoria di cui all'art. 25 e, ove prescritta, nella valutazione d'impatto di cui all'art. 12.

Art. 6 – Finalità del trattamento

1. Le finalità perseguite mediante i sistemi di videosorveglianza sono conformi alle funzioni istituzionali attribuite al Comune dalla legge, dallo Statuto e dai regolamenti, e sono precisamente individuate tra le seguenti:

a) protezione e incolumità delle persone e tutela della sicurezza urbana, ai sensi e nei limiti del D.L. 14/2017, conv. in L. 48/2017, e del successivo art. 21;

b) prevenzione e repressione di atti delittuosi, di atti di vandalismo e di danneggiamento del patrimonio comunale, e tutela dei beni e degli immobili di proprietà o in uso all'Ente;

c) rilevazione, anche in tempo reale, di situazioni di congestione o pericolo per la circolazione stradale, al fine di consentire il pronto intervento della Polizia Locale, nonché monitoraggio dei flussi di traffico;

d) controllo degli accessi veicolari in zone a traffico limitato o in aree determinate del territorio comunale, nel rispetto della normativa vigente in materia;

e) controllo di aree pubbliche abusivamente utilizzate quali discariche di materiali e di sostanze pericolose, e accertamento degli illeciti in materia ambientale e di abbandono di rifiuti;

f) controllo di aree pubbliche a rischio a fini di protezione civile, previa individuazione nel relativo Piano;

g) agevolazione dell'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del Comune o di terzi sulla base di immagini utili in caso di fatti illeciti.

2. È vietato utilizzare i sistemi di videosorveglianza per finalità diverse da quelle indicate al comma 1 e comunque per finalità di controllo a distanza dell'attività lavorativa dei dipendenti. Ove dall'installazione derivi anche la possibilità di controllo indiretto dei lavoratori, trovano applicazione le garanzie di cui all'art. 4 della L. 300/1970, come modificato dal D.Lgs. 151/2015, ivi compreso, ove prescritto, il previo accordo sindacale o l'autorizzazione dell'Ispettorato territoriale del lavoro.

3. L'individuazione delle aree interessate dalla videosorveglianza e delle modalità di effettuazione delle riprese è disposta dalla Giunta comunale con proprio atto deliberativo, nell'ambito delle finalità di cui al comma 1 e previa istruttoria conforme all'art. 25.

CAPO II – SOGGETTI, ADEMPIMENTI E RESPONSABILITÀ

Art. 7 – Titolare del trattamento

1. Titolare del trattamento è il Comune di Villar Pellice, rappresentato dal Sindaco pro tempore quale legale rappresentante dell'Ente.

2. Il Titolare, in attuazione del principio di responsabilizzazione, mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR, riesaminandole e aggiornandole ove necessario (art. 24 GDPR).

3. È abrogato ogni adempimento di notificazione preventiva o di verifica preliminare al Garante già previsto dagli artt. 17 e 37 del Codice nel testo anteriore al D.Lgs. 101/2018; tali istituti sono sostituiti dalla valutazione d'impatto di cui all'art. 12 e, ove ne ricorrano i presupposti, dalla consultazione preventiva ai sensi dell'art. 36 GDPR.

Art. 8 – Responsabile della protezione dei dati (RPD/DPO)

1. Il Comune, in quanto autorità pubblica, ha designato il Responsabile della protezione dei dati ai sensi dell'art. 37, par. 1, lett. a), GDPR, i cui dati di contatto sono pubblicati sul sito istituzionale e comunicati al Garante.

2. Il RPD è tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la videosorveglianza, e in particolare: nell'istruttoria per l'installazione di nuovi impianti o l'estensione di quelli esistenti; nella redazione e revisione della valutazione d'impatto di

cui all'art. 12, della quale è obbligatoriamente acquisito il parere ai sensi dell'art. 35, par. 2, GDPR; nella gestione delle istanze degli interessati e delle violazioni di dati personali.

Art. 9 – Soggetti autorizzati al trattamento e amministratori di sistema

1. Il Titolare, anche per il tramite dei dirigenti/responsabili di servizio a ciò designati ai sensi dell'art. 2-quaterdecies del Codice, ed in particolare del Responsabile della Polizia Locale, individuato quale soggetto designato, autorizza per iscritto e in numero limitato le persone fisiche addette al trattamento dei dati, all'utilizzo degli impianti e, nei soli casi in cui risulti indispensabile per gli scopi perseguiti, alla visione delle registrazioni.

2. L'atto di autorizzazione individua analiticamente l'ambito del trattamento consentito, i compiti affidati e le istruzioni impartite ai sensi dell'art. 29 GDPR. I soggetti autorizzati sono vincolati alla riservatezza e adeguatamente formati, con percorsi di formazione iniziale e di aggiornamento periodico in materia di protezione dei dati personali.

3. I soggetti che, nell'ambito della gestione tecnica degli impianti, rivestono funzioni di amministratore di sistema sono designati individualmente, con elencazione degli ambiti di operatività consentiti, nel rispetto del Provvedimento del Garante del 27 novembre 2008. I loro accessi logici sono oggetto di registrazione (access log) con conservazione degli stessi per almeno sei mesi e di verifica almeno annuale dell'operato.

Art. 10 – Responsabili del trattamento ex art. 28 GDPR

1. Qualora attività di trattamento siano affidate a soggetti esterni – quali la ditta installatrice, la società incaricata della manutenzione del sistema, il fornitore di servizi di conservazione o gestione delle immagini, l'eventuale istituto di vigilanza – tali soggetti sono designati Responsabili del trattamento mediante contratto o altro atto giuridico conforme all'art. 28 GDPR, che disciplina la materia, la durata, la natura e la finalità del trattamento, il tipo di dati personali, le categorie di interessati, gli obblighi e i diritti del Titolare.

2. Il ricorso a eventuali sub-responsabili è soggetto ad autorizzazione scritta del Titolare. L'accesso alle immagini da parte del personale del Responsabile è consentito nei soli limiti strettamente necessari al compimento delle funzioni assegnate.

Art. 11 – Registro delle attività di trattamento

1. Il trattamento effettuato mediante i sistemi di videosorveglianza è censito nel Registro delle attività di trattamento tenuto dal Titolare ai sensi dell'art. 30 GDPR, con indicazione, tra l'altro, delle finalità, delle categorie di interessati e di dati, dei destinatari, dei termini di cancellazione e della descrizione generale delle misure di sicurezza.

2. Il Registro è aggiornato in occasione di ogni modifica rilevante degli impianti o delle modalità del trattamento.

Art. 12 – Valutazione d'impatto sulla protezione dei dati (DPIA)

1. La sorveglianza sistematica su larga scala di zone accessibili al pubblico rientra tra i trattamenti per i quali l'art. 35, par. 3, lett. c), GDPR prescrive la valutazione d'impatto sulla protezione dei dati; il trattamento è altresì ricompreso nell'elenco delle tipologie soggette a DPIA adottato dal Garante con provvedimento n. 467 dell'11 ottobre 2018.

2. Prima dell'attivazione di nuovi impianti, dell'estensione significativa di quelli esistenti o dell'introduzione di nuove tecnologie (ivi compresi sistemi di analisi video evoluta), il Titolare effettua la DPIA, contenente la descrizione sistematica dei trattamenti, la valutazione della necessità e proporzionalità, la valutazione dei rischi per i diritti e le libertà degli interessati e le misure previste per affrontarli.

3. Qualora dalla DPIA emerga un rischio residuo elevato non adeguatamente mitigabile, il Titolare consulta preventivamente il Garante ai sensi dell'art. 36 GDPR prima di procedere al trattamento.

4. La DPIA è riesaminata periodicamente e, comunque, in occasione di ogni variazione dei rischi rappresentati dal trattamento.

CAPO III – MODALITÀ DEL TRATTAMENTO

Art. 13 – Informativa agli interessati

1. Gli interessati sono informati, ai sensi degli artt. 12 e 13 GDPR e secondo il modello a doppio livello raccomandato dalle Linee guida EDPB 3/2019 e dal Garante, dell'ingresso o della presenza in una zona videosorvegliata e dell'eventuale registrazione.

2. L'informativa di primo livello (cartello di area videosorvegliata) è resa mediante segnaletica conforme al modello di cui all'Allegato A, collocata prima del raggio d'azione delle telecamere o nelle sue immediate vicinanze, chiaramente visibile anche in condizioni di scarsa illuminazione qualora l'impianto sia attivo in orario notturno. Il cartello riporta almeno: il simbolo della telecamera; l'identità del Titolare; le finalità del trattamento; l'esistenza della registrazione e i tempi di conservazione; il riferimento ai diritti degli interessati; i dati di contatto del Titolare e del RPD; le modalità per reperire l'informativa completa.

3. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, sono installati più cartelli.

4. L'informativa completa di secondo livello, contenente tutti gli elementi di cui all'art. 13 GDPR, è pubblicata sul sito internet istituzionale del Comune ed è resa disponibile, su richiesta, presso gli uffici comunali.

5. Il Titolare rende noti alla comunità cittadina, con appositi avvisi da pubblicare sul sito internet istituzionale e all'Albo Pretorio on line, l'attivazione dei sistemi di videosorveglianza, l'eventuale incremento dimensionale degli impianti e l'eventuale cessazione del trattamento.

Art. 14 – Modalità di raccolta delle immagini e requisiti degli impianti

1. I dati personali sono raccolti mediante sistemi di ripresa a circuito chiuso installati in prossimità degli immobili di proprietà comunale, in corrispondenza delle principali vie di comunicazione e relativi incroci, di parchi e luoghi pubblici, di aree a rischio a fini di protezione civile o interessate da fenomeni di abbandono di rifiuti, secondo l'elenco dei siti di ripresa approvato dalla Giunta comunale.

2. Il sistema garantisce, mediante idonee funzioni di privacy masking, l'oscuramento automatico e irreversibile delle zone relative ad aree private (ingressi, finestre, pertinenze

di abitazioni ed esercizi) e delle porzioni di territorio non pertinenti rispetto alle finalità perseguite.

3. Le telecamere possono consentire riprese a colori o in bianco/nero, essere dotate di brandeggio e zoom ottico programmati e collegate a un centro di gestione e archiviazione che può, esclusivamente per il perseguimento dei fini istituzionali, digitalizzare o indicizzare le immagini.

4. Fatto salvo quanto previsto dagli artt. 22 e 23, i sistemi installati non consentono trattamenti di analisi video evoluta idonei a rilevare automaticamente caratteristiche fisionomiche o biometriche delle persone, a ricostruirne i percorsi, a classificarne il comportamento o a generare allarmi su base comportamentale, salvo che tali funzionalità siano state oggetto di specifica valutazione d'impatto favorevole, risultino conformi al Regolamento (UE) 2024/1689 e siano state espressamente autorizzate con l'atto deliberativo di cui all'art. 6, comma 3.

5. I segnali video sono raccolti presso la centrale di controllo ubicata nella Sede Municipale o in altra sede idonea. I monitor sono collocati in locale con visuale non accessibile al pubblico; il sistema di registrazione è collocato in locale ad accesso riservato al solo personale autorizzato. Le immagini sono registrate in formato digitale su supporti protetti; l'eventuale replica dei dati per finalità di continuità operativa è ammessa nei soli limiti in cui sia ricompresa nelle misure di sicurezza documentate e non comporti duplicazioni eccedenti i tempi di conservazione di cui all'art. 15.

6. L'accesso remoto alle immagini, ove previsto, avviene esclusivamente mediante canali cifrati e autenticazione forte, ed è tracciato.

Art. 15 – Conservazione e cancellazione dei dati

1. In applicazione del principio di limitazione della conservazione, le immagini registrate sono conservate per il tempo strettamente necessario e comunque, in via ordinaria, per un periodo non superiore a settantadue (72) ore successive alla rilevazione, tenuto conto della necessità di garantire idonei tempi di verifica in relazione a festività o chiusura di uffici o servizi. La congruità del predetto termine rispetto alle finalità perseguite è motivata nella valutazione d'impatto di cui all'art. 12.

2. Per gli impianti attivati per finalità di sicurezza urbana ai sensi dell'art. 21, il termine di conservazione può essere elevato fino a sette giorni, ove ciò risulti necessario e proporzionato in relazione alle specifiche esigenze documentate nella DPIA, salvo speciali esigenze di ulteriore conservazione previste dalla legge.

3. Al termine del periodo stabilito, il sistema provvede in automatico alla cancellazione delle immagini mediante sovraregistrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

4. Un eventuale allungamento dei tempi di conservazione è consentito in via eccezionale, in relazione alla necessità derivante da un evento già accaduto o realmente incombente, ovvero alla necessità di custodire o consegnare copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso; in tali casi la conservazione è limitata alle sole immagini pertinenti.

5. Le immagini estratte e riversate su supporti rimovibili per la consegna alle forze di polizia o ai soggetti legittimati sono conservate in cassaforte presso gli uffici comunali, in spazio accessibile esclusivamente ai soggetti autorizzati, e i supporti non più necessari sono distrutti in modo sicuro.

6. In caso di sostituzione o dismissione dei supporti di memorizzazione, questi sono cancellati in modo sicuro o distrutti fisicamente, in modo da rendere impossibile il recupero dei dati.

7. Nel caso in cui si verifichino furti, atti di vandalismo o eventi comunque lesivi del patrimonio dell'Ente, è consentita, su disposizione del soggetto a ciò autorizzato e limitatamente alle riprese di specifico interesse e attinenza con i fatti, l'estrazione e la conservazione delle immagini e il loro utilizzo nel procedimento di accertamento e contestazione dell'illecito e per l'esercizio del diritto di difesa.

Art. 16 – Misure di sicurezza

1. Ai sensi dell'art. 32 GDPR, tenuto conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà degli interessati, il Titolare e i Responsabili mettono in atto misure

tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, tra cui in particolare:

a) sistemi di autenticazione individuale degli operatori, con credenziali personali e, per gli accessi remoti o privilegiati, autenticazione a più fattori;

b) profili di autorizzazione differenziati (visione live, visione del registrato, estrazione), attribuiti secondo il principio del minimo privilegio e riesaminati periodicamente;

c) registrazione (log) degli accessi al sistema e delle operazioni di visione ed estrazione delle immagini, con conservazione dei log per un periodo congruo;

d) cifratura dei flussi video trasmessi su reti pubbliche o non dedicate e protezione delle reti mediante segregazione, firewall e aggiornamento costante di firmware e software degli apparati;

e) modifica delle credenziali predefinite di fabbrica di tutti i dispositivi e disattivazione dei servizi non necessari;

f) collocazione degli apparati di registrazione in locali protetti e ad accesso controllato;

g) procedure di verifica periodica dell'integrità e del corretto funzionamento del sistema, ivi compresi i tempi di cancellazione automatica.

2. All'atto dell'installazione o di interventi di manutenzione evolutiva, è acquisita dall'installatore una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni vigenti e alle misure di sicurezza adottate.

Art. 17 – Violazioni di dati personali (data breach)

1. In caso di violazione dei dati personali riferita ai sistemi di videosorveglianza (a titolo esemplificativo: accesso abusivo alla centrale o ai flussi video, perdita o sottrazione di supporti, diffusione non autorizzata di immagini), il soggetto che ne viene a conoscenza informa senza ritardo il Titolare e il RPD, secondo la procedura interna di gestione delle violazioni adottata dall'Ente.

2. Il Titolare, ove ne ricorrano i presupposti, notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza (art. 33 GDPR) e, quando la violazione è suscettibile di presentare un rischio

elevato per i diritti e le libertà delle persone fisiche, la comunica agli interessati (art. 34 GDPR). Tutte le violazioni sono documentate nell'apposito registro interno.

Art. 18 – Obblighi degli operatori

1. L'utilizzo delle telecamere è consentito solo per la sorveglianza di quanto si svolge nelle aree pubbliche o aperte al pubblico individuate negli atti deliberativi, per le finalità di cui all'art. 6.

2. Fatti salvi i casi di esercizio dei diritti da parte degli interessati, le immagini registrate possono essere riesaminate, nel limite del tempo di conservazione ammesso, solo dai soggetti a ciò autorizzati, in caso di effettiva necessità e per l'esclusivo perseguimento delle finalità istituzionali.

3. È fatto divieto agli operatori di effettuare riprese di dettaglio non pertinenti, di utilizzare le funzioni di brandeggio e zoom per inquadrare aree private o soggetti determinati al di fuori delle necessità operative, di duplicare, comunicare o diffondere le immagini al di fuori dei casi previsti dal presente Regolamento e dalla legge, nonché di effettuare riprese o estrazioni mediante dispositivi personali.

4. La mancata osservanza degli obblighi di cui al presente articolo comporta l'applicazione delle sanzioni disciplinari previste dai vigenti CCNL e codici di comportamento, ferma restando l'eventuale responsabilità amministrativa, civile e penale.

CAPO IV – DIRITTI DELL'INTERESSATO E COMUNICAZIONE DEI DATI

Art. 19 – Diritti dell'interessato

1. L'interessato può esercitare, nei confronti del Titolare, i diritti previsti dagli artt. 15-22 GDPR, in quanto compatibili con la natura del trattamento, e in particolare:

a) il diritto di accesso (art. 15 GDPR), ossia di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, l'accesso ai dati e alle informazioni previste dalla norma, ivi compresa copia delle immagini che lo riguardano, con oscuramento dei terzi eventualmente ripresi;

b) il diritto di cancellazione (art. 17 GDPR) e il diritto di limitazione del trattamento (art. 18 GDPR), nei casi previsti;

c) il diritto di opposizione (art. 21 GDPR), per motivi connessi alla sua situazione particolare, al trattamento fondato sull'art. 6, par. 1, lett. e), GDPR.

2. In ragione della natura del trattamento, non trovano applicazione il diritto di rettifica e il diritto alla portabilità dei dati; il diritto di cancellazione non può essere esercitato in pregiudizio delle esigenze di accertamento di illeciti o di difesa in giudizio.

3. L'istanza è presentata al Titolare, anche per il tramite del RPD, mediante consegna a mano all'Ufficio Protocollo, raccomandata, posta elettronica ordinaria o certificata. Per consentire l'individuazione delle immagini, la richiesta indica l'impianto cui si fa riferimento, il giorno e l'ora della ripresa e ogni ulteriore elemento utile; alla richiesta sono allegati copia di un documento di identità e, ove necessario per l'identificazione nelle riprese, una fotografia del richiedente.

4. Il Titolare fornisce riscontro senza ingiustificato ritardo e, comunque, entro un mese dal ricevimento dell'istanza, prorogabile di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste, dandone comunicazione motivata all'interessato entro il primo mese (art. 12, par. 3, GDPR). Qualora le immagini risultino già cancellate per decorso dei termini di conservazione, il riscontro ne dà atto.

5. L'esercizio dei diritti è gratuito, salvo il caso di richieste manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, nel qual caso il Titolare può addebitare un contributo spese ragionevole ovvero rifiutare di soddisfare la richiesta, motivando il diniego.

6. In caso di riscontro ritenuto non satisfattivo o di mancato riscontro, l'interessato può proporre reclamo al Garante ai sensi dell'art. 77 GDPR e degli artt. 140-bis e ss. del Codice, ovvero ricorso all'autorità giurisdizionale.

7. I diritti riferiti ai dati personali concernenti persone decedute possono essere esercitati, ai sensi dell'art. 2-terdecies del Codice, da chi ha un interesse proprio o agisce a tutela dell'interessato in qualità di suo mandatario o per ragioni familiari meritevoli di protezione.

Art. 20 – Comunicazione dei dati e accesso da parte dell'autorità giudiziaria e delle forze di polizia

1. La comunicazione di dati personali da parte del Comune ad altri soggetti pubblici è ammessa, ai sensi dell'art. 2-ter del Codice, quando prevista da una norma di legge o di regolamento ovvero quando risulti comunque necessaria per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

2. Le immagini sono messe a disposizione dell'autorità giudiziaria e della polizia giudiziaria a fronte di richiesta o provvedimento formale, con estrazione limitata alle riprese pertinenti e verbalizzazione della consegna. L'accesso in tempo reale ai flussi video da parte delle Forze di Polizia dello Stato è disciplinato dagli accordi di cui all'art. 21.

3. La comunicazione di dati personali a privati è ammessa unicamente quando prevista da una norma di legge o nei casi di esercizio del diritto di difesa, nei limiti strettamente necessari. È in ogni caso vietata la diffusione delle immagini.

4. L'accesso alle immagini da parte della ditta installatrice o incaricata della manutenzione, designata ai sensi dell'art. 10, è consentito nei soli limiti strettamente necessari alle specifiche funzioni assegnate.

5. Le istanze di accesso documentale ex L. 241/1990 e di accesso civico generalizzato ex D.Lgs. 33/2013 aventi ad oggetto le immagini sono valutate nel rispetto dei limiti posti a tutela della protezione dei dati personali dei terzi e delle esigenze di ordine e sicurezza pubblica, sentito ove opportuno il RPD.

CAPO V – TRATTAMENTI PARTICOLARI

Art. 21 – Videosorveglianza per finalità di sicurezza urbana e controllo integrato del territorio

1. Nell'ambito delle politiche di sicurezza integrata e di sicurezza urbana di cui al D.L. 14/2017, conv. in L. 48/2017, il Comune può attivare o potenziare sistemi di videosorveglianza in attuazione dei patti per la sicurezza urbana sottoscritti con il Prefetto, ai sensi dell'art. 5, comma 2, lett. a), del medesimo decreto, anche ai fini dell'accesso ai finanziamenti statali previsti dall'art. 5, comma 2-ter.

2. Al fine di rilevare in tempo reale situazioni di pericolo per la sicurezza pubblica o il verificarsi di condizioni di emergenza che legittimino l'intervento delle Forze di Polizia

statali, il Comune attua politiche di controllo integrato del territorio, anche mediante il collegamento dei propri impianti con le sale operative delle Forze di Polizia, previa formalizzazione di appositi protocolli o convenzioni che definiscano ruoli, responsabilità, modalità di accesso e misure di sicurezza.

3. I dati raccolti nell'ambito del presente articolo possono essere utilizzati esclusivamente dalle autorità e dagli organi istituzionalmente preposti alla prevenzione e repressione di atti delittuosi, nel rispetto del D.Lgs. 51/2018 per i trattamenti di rispettiva competenza.

4. Il Comune può altresì aderire a iniziative di videosorveglianza sovracomunali, in forma associata o convenzionata con altri enti locali, previa definizione, con apposito atto, della contitolarità ai sensi dell'art. 26 GDPR ovvero dei distinti ruoli di titolarità e responsabilità del trattamento.

Art. 22 – Sistemi di lettura automatica delle targhe (ANPR/LPR)

1. L'eventuale installazione di dispositivi di rilevazione e lettura automatica delle targhe dei veicoli in transito è consentita esclusivamente per le finalità istituzionali di cui all'art. 6 e nei limiti delle attribuzioni della Polizia Locale, previa specifica valutazione d'impatto ai sensi dell'art. 12, trattandosi di monitoraggio sistematico su larga scala.

2. I dispositivi sono configurati in modo da limitare la raccolta ai dati strettamente necessari (targa, data, ora, varco), da escludere interrogazioni massive non pertinenti e da garantire tempi di conservazione differenziati e proporzionati alle singole finalità, come definiti nella DPIA e negli atti attuativi.

3. L'eventuale interconnessione con banche dati esterne (a titolo esemplificativo: veicoli rubati o privi di copertura assicurativa) è ammessa nei soli casi previsti dalla legge e con modalità tracciate.

Art. 23 – Divieto di identificazione biometrica e sistemi di intelligenza artificiale

1. È vietata l'installazione e l'utilizzazione, sugli impianti disciplinati dal presente Regolamento, di sistemi di riconoscimento facciale e, in generale, di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico, in conformità all'art. 5, par. 1, lett. h), del Regolamento (UE) 2024/1689, ferme restando le

eccezioni tassative ivi previste, riservate alle autorità di contrasto alle condizioni e con le autorizzazioni prescritte dal medesimo Regolamento e dalla normativa nazionale di adeguamento, e comunque estranee alle competenze comunali.

2. Sono altresì vietati, ai sensi dell'art. 5 del Regolamento (UE) 2024/1689: i sistemi di categorizzazione biometrica che deducono caratteristiche sensibili delle persone; i sistemi di riconoscimento delle emozioni nei luoghi di lavoro; la creazione o l'ampliamento di banche dati di riconoscimento facciale mediante estrazione non mirata (scraping) di immagini da Internet o da filmati di videosorveglianza.

3. L'eventuale futura adozione di funzionalità di analisi video basate su sistemi di intelligenza artificiale non ricadenti nei divieti di cui ai commi precedenti è subordinata: alla classificazione del sistema e all'adempimento degli obblighi previsti dal Regolamento (UE) 2024/1689, ivi compresi, per i sistemi ad alto rischio, gli obblighi dell'utilizzatore (deployer) di cui all'art. 26 e la valutazione d'impatto sui diritti fondamentali di cui all'art. 27, ove prescritta; alla valutazione d'impatto sulla protezione dei dati di cui all'art. 12; alla conformità alla L. 132/2025 e ai provvedimenti delle autorità nazionali competenti; a espressa deliberazione autorizzativa della Giunta comunale.

Art. 24 – Impianti temporanei e mobili

1. Per specifiche e documentate esigenze (manifestazioni, cantieri, fenomeni di abbandono di rifiuti, situazioni contingenti di degrado o pericolo), possono essere attivati impianti di videosorveglianza temporanei o rilocabili, comprese fototrappole e droni, nel rispetto dei principi e delle garanzie del presente Regolamento, con individuazione preventiva della durata, dell'area interessata e delle finalità, e previa adozione di apposito Disciplinare di utilizzo da parte del Responsabile della Polizia Locale.

2. Anche per gli impianti temporanei è assicurata l'informativa di cui all'art. 13, salvo quanto diversamente previsto dalla normativa vigente per gli accertamenti di illeciti in materia ambientale, nei limiti chiariti dal Garante.

CAPO VI – NORME FINALI

Art. 25 – Provvedimenti attuativi

1. Compete alla Giunta comunale, sulla scorta di istruttoria idonea a dimostrare il rispetto dei principi e delle modalità prescritte dal presente Regolamento – ivi compresi gli esiti della valutazione d'impatto ove prescritta e il coinvolgimento del RPD – l'assunzione dei provvedimenti attuativi conseguenti, con particolare riferimento all'individuazione, modifica o integrazione dell'elenco dei siti di ripresa, sia permanenti sia temporanei, all'eventuale fissazione degli orari delle registrazioni, nonché alla definizione di ogni ulteriore disposizione ritenuta utile.

Art. 26 – Sanzioni

1. La violazione delle disposizioni in materia di protezione dei dati personali è soggetta alle sanzioni amministrative pecuniarie di cui all'art. 83 GDPR, applicate dal Garante secondo i criteri di cui all'art. 166 del Codice, ferme restando le fattispecie penali di cui agli artt. 167 e ss. del Codice e la responsabilità disciplinare, amministrativo-contabile e civile del personale.

Art. 27 – Norme di rinvio e adeguamento automatico

1. Per quanto non disciplinato dal presente Regolamento, si rinvia al Regolamento (UE) 2016/679, al D.Lgs. 196/2003 e s.m.i., al D.Lgs. 51/2018, al Regolamento (UE) 2024/1689, alla L. 132/2025, nonché ai provvedimenti generali, alle linee guida e alle FAQ adottati dal Garante per la protezione dei dati personali e dal Comitato europeo per la protezione dei dati in materia di videosorveglianza.

2. Le successive modifiche e integrazioni della normativa europea e nazionale in materia, nonché i provvedimenti precettivi e vincolanti delle autorità competenti, si intendono automaticamente recepiti dal presente Regolamento, che sarà comunque adeguato ove necessario.

Art. 28 – Pubblicità del Regolamento

1. Copia del presente Regolamento è pubblicata in via permanente sul sito internet istituzionale del Comune, nella sezione "Amministrazione trasparente", ed è tenuta a disposizione del pubblico affinché chiunque possa prenderne visione in qualsiasi momento.

2. Copia dello stesso è trasmessa al Responsabile della protezione dei dati, al Responsabile del Servizio di Polizia Locale e ai Responsabili degli Uffici comunali interessati.

Art. 29 – Abrogazioni ed entrata in vigore

1. Il presente Regolamento, divenuta esecutiva la deliberazione consiliare di approvazione, è pubblicato per quindici giorni all'Albo Pretorio on line ed entra in vigore l'ultimo giorno di pubblicazione.

2. Dalla data di entrata in vigore del presente Regolamento è abrogato ogni regolamentazione precedente e incompatibile con le presenti disposizioni.

COMUNE DI VILLAR PELLICE - Prot 0006396 del 22/10/2026 Tit 1 Cl 1 Fasc

ALLEGATO A

Modello di informativa minima – Cartello di area videosorvegliata

(conforme al modello EDPB – Linee guida 3/2019 e al Provvedimento del Garante del 26 novembre 2020)

AREA VIDEOSORVEGLIATA

[simbolo grafico della telecamera]

La registrazione è effettuata per le seguenti finalità: sicurezza urbana, tutela del patrimonio comunale e delle persone, controllo del territorio.

Titolare del trattamento: Comune di Villar Pellice – [indirizzo] – tel. [___] – PEC: [___]

Responsabile della protezione dei dati (RPD/DPO): [nominativo/società] – e-mail: [___]

Conservazione delle immagini: le immagini registrate sono conservate per un massimo di [72 ore / 7 giorni], salvo specifiche richieste dell'autorità giudiziaria o di polizia giudiziaria.

Diritti degli interessati: gli interessati possono esercitare i diritti previsti dagli artt. 15 e ss. del Regolamento (UE) 2016/679, rivolgendosi al Titolare o al RPD.

Informativa completa: disponibile sul sito www.comune.villarpellice.to.it e presso gli uffici comunali.

Note di installazione: il cartello deve essere collocato prima del raggio d'azione delle telecamere o nelle sue immediate vicinanze, in posizione chiaramente visibile; deve essere visibile anche in condizioni di scarsa illuminazione qualora l'impianto sia attivo in orario notturno; in presenza di più telecamere, in relazione alla vastità dell'area, devono essere installati più cartelli.